Guide d'installation

McAfee Enterprise Security Manager 9.5.0

COPYRIGHT

Copyright © 2015 McAfee, Inc., 2821 Mission College Boulevard, Santa Clara, CA 95054, 1.888.847.8766, www.intelsecurity.com

DROITS DE MARQUES

Intel et le logo Intel sont des marques commerciales déposées d'Intel Corporation aux États-Unis et/ou dans d'autres pays. McAfee et le logo McAfee, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Evader, Foundscore, Foundstone, Global Threat Intelligence, McAfee LiveSafe, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee TechMaster, McAfee Total Protection, TrustedSource, VirusScan sont des marques commerciales ou des marques commerciales déposées de McAfee, Inc. ou de ses filiales aux États-Unis et dans d'autres pays. Les autres noms et marques sont la propriété de leurs détenteurs respectifs.

INFORMATIONS DE LICENCE

Accord de licence

À L'ATTENTION DE TOUS LES UTILISATEURS : VEUILLEZ LIRE ATTENTIVEMENT L'ACCORD LÉGAL APPROPRIÉ CORRESPONDANT À LA LICENCE QUE VOUS AVEZ ACHETÉE, QUI DÉFINIT LES CONDITIONS GÉNÉRALES D'UTILISATION DU LOGICIEL SOUS LICENCE. SI VOUS NE CONNAISSEZ PAS LE TYPE DE LICENCE QUE VOUS AVEZ ACQUIS, CONSULTEZ LES DOCUMENTS DE VENTE, D'ATTRIBUTION DE LICENCE OU LE BON DE COMMANDE QUI ACCOMPAGNENT LE LOGICIEL OU QUE VOUS AVEZ REÇUS SÉPARÉMENT LORS DE L'ACHAT (SOUS LA FORME D'UN LIVRET, D'UN FICHIER SUR LE CD-ROM DU PRODUIT OU D'UN FICHIER DISPONIBLE SUR LE SITE WEB À PARTIR DUQUEL VOUS AVEZ TÉLÉCHARGÉ LE PACKAGE LOGICIEL). SI VOUS N'ACCEPTEZ PAS TOUTES LES DISPOSITIONS DE CET ACCORD, NE PROCÉDEZ PAS À L'INSTALLATION DU LOGICIEL. LE CAS ÉCHÉANT, VOUS POUVEZ RETOURNER LE PRODUIT À MCAFEE OU À VOTRE REVENDEUR AFIN D'EN OBTENIR LE REMBOURSEMENT INTÉGRAL

Sommaire

Préface **5**
Présentation de ce guide 5
Public visé 5
Conventions 5
Accès à la documentation sur le produit 6

1 Présentation **7**

2 Installation des équipements McAfee ESM **9**
Préparation de l'installation des équipements McAfee ESM 9
Configuration matérielle et logicielle requise 9
Inspection de l'emballage et de l'équipement 10
Identification d'un emplacement pour l'installation 10
Connexion et démarrage des équipements 11
Identification des types de connecteur et d'équipement 12
Identification des câbles réseau 12
Identification des ports réseau 13

3 Configuration des équipements McAfee ESM **23**
Configuration de l'interface réseau dans Nitro IPS 23
Configuration de l'interface réseau dans Receiver, ELM et ACE 24
Configuration de l'interface réseau dans DEM et ADM 24
Configuration de l'interface réseau dans ESM 25
Configuration du protocole IPv6 26
Connexion à la console McAfee ESM 26

A A propos du mode FIPS **29**
Informations sur le mode FIPS 30
Sélection du mode FIPS 30
Vérification de l'intégrité FIPS 31
Ajout d'un équipement dont la clé est activée en mode FIPS 32
Sauvegarde et restauration des informations d'un équipement en mode FIPS 32
Activation de la communication avec plusieurs équipements ESM en mode FIPS 33
Résolution des problèmes liés au mode FIPS 35

B Configuration requise pour une machine virtuelle ESXi **37**
Modèles de machine virtuelle (VM) 37
Agrégation par bandes du lecteur de stockage 39
Installation de la machine virtuelle 40
Configuration de la machine virtuelle 41
Activation de la clé de l'équipement virtuel 41

C Installation de la carte réseau SAN qLogic 2460 ou 2562 **43**

D Installation de DAS **45**

E Installation des équipements dans un rack **47**
Installation du kit de rails AXXVRAIL 48
Retrait du châssis 51

F Avis réglementaires **53**

Index **57**

Préface

Ce guide fournit les informations dont vous avez besoin pour utiliser votre produit McAfee.

Sommaire

- *Présentation de ce guide*
- *Accès à la documentation sur le produit*

Présentation de ce guide

Cette section présente le public ciblé par ce guide, les conventions typographiques et les icônes utilisées ainsi que la structure du guide.

Public visé

La documentation McAfee a fait l'objet de recherches attentives et a été rédigée en fonction du public visé.

Les informations présentées dans ce guide sont principalement destinées aux personnes suivantes :

- **Administrateurs** : personnes qui mettent en œuvre et appliquent le programme de sécurité de l'entreprise.
- **Utilisateurs** : personnes qui utilisent l'ordinateur sur lequel le logiciel est exécuté et peuvent accéder à certaines ou toutes ses fonctionnalités.

Conventions

Les conventions typographiques et icônes suivantes sont respectées dans le présent guide.

Titre du manuel, *terme*, *accentuation*	Titre d'un manuel, chapitre ou rubrique ; nouveau terme ; accentuation.
Gras	Texte mis en évidence de manière particulière.
`Entrée utilisateur, code, message`	Commandes et autre texte saisi par l'utilisateur ; exemple de code ; message affiché.
Texte d'interface	Termes de l'interface du produit, par exemple les options, menus, boutons et boîtes de dialogue.
Lien hypertexte bleu	Lien actif vers une rubrique ou un site web externe.
	Remarque : Informations complémentaires, par exemple un autre moyen d'accéder à une option.
	Conseil : Suggestions et recommandations.

Important/Attention : Conseil important visant à protéger un système informatique, l'installation d'un logiciel, un réseau ou des données.

Avertissement : Conseil crucial visant à empêcher les dommages corporels lors de l'utilisation du matériel informatique.

Accès à la documentation sur le produit

Dès qu'un produit est distribué, les informations le concernant sont intégrées dans le Centre de connaissances en ligne de McAfee.

Procédure

1. Accédez à l'onglet **Centre de connaissances** du portail McAfee ServicePortal à l'adresse http://support.mcafee.com.
2. Dans le volet **Base de connaissances**, cliquez sur une source de contenu :
   - **Documentation produit** pour rechercher une documentation utilisateur
   - **Articles techniques** pour rechercher des articles de la base de connaissances
3. Sélectionnez **Ne pas effacer mes filtres**.
4. Entrez un produit, sélectionnez une version, puis cliquez sur **Rechercher** pour afficher une liste de documents.

1 Présentation

Ce guide explique comment installer et configurer les équipements suivants :

- McAfee® Nitro Intrusion Prevention System (IPS)
- McAfee® Enterprise Security Manager (McAfee ESM)
- McAfee Event Receiver
- McAfee ESM/Event Receiver (ESMREC)
- McAfee Database Event Monitor (DEM)
- McAfee Application Data Monitor (ADM)
- McAfee Enterprise Log Manager (ELM)
- McAfee Advanced Correlation Editor (ACE)
- McAfee Direct Attached Storage (DAS)
- McAfee Receiver/ELM (ELMERC)
- McAfee ESM/Receiver/ELM (ESMELM)

Il est divisé en deux sections principales :

- Installation d'un équipement McAfee ESM, qui vous indique les étapes à suivre pour inspecter, monter, connecter et démarrer l'équipement.
- Configuration d'un équipement McAfee ESM, qui décrit les procédures à suivre pour configurer l'interface réseau de chaque type d'équipement, configurer le protocole IPv6, se connecter à la console McAfee ESM et activer la clé de l'équipement.

1 Présentation

2 Installation des équipements McAfee ESM

Vous devez installer vos équipements McAfee avant de pouvoir les utiliser pour protéger votre réseau des intrusions ou pour collecter des données réseau. Ces instructions d'installation s'appliquent à tous les modèles actuels des équipements McAfee ESM.

Sommaire

- *Préparation de l'installation des équipements McAfee ESM*
- *Connexion et démarrage des équipements*

Préparation de l'installation des équipements McAfee ESM

Avant d'installer des équipements, vérifiez que votre système est conforme à la configuration minimale requise et que l'équipement n'a pas été endommagé durant le transport. Sélectionnez l'emplacement de configuration de l'équipement.

Configuration matérielle et logicielle requise

Votre système doit être conforme à la configuration matérielle et logicielle requise minimale.

Configuration système requise

- Processeur : classe P4 (autre que Celeron) ou supérieure (Mobile/Xeon/Core 2, Core i3/5/7) ou classe AMD AM2 ou supérieure (Turion 64/Athlon 64/Opteron 64, A4/6/8)
- RAM : 1,5 Go
- Système d'exploitation Windows : Windows 2000, Windows XP, Windows 2003 Server, Windows Vista, Windows 2008 Server, Windows Server 2012, Windows 7, Windows 8, Windows 8.1
- Navigateur : Internet Explorer 7.x ou ultérieur, Mozilla Firefox 3.0.0.0 ou ultérieur, Google Chrome 12.0.742.91 ou ultérieur
- Flash Player : version 11.2.x.x ou ultérieure

Les fonctionnalités d'ESM affichent des fenêtres pop-up lors du chargement ou du téléchargement des fichiers. Désactivez le blocage des fenêtres pop-up pour l'adresse IP ou le nom d'hôte de votre ESM.

Configuration requise pour une machine virtuelle

- Processeur : 8 cœurs 64 bits, Dual Core 2/Nehalem ou supérieur ou AMD Dual Athlon 64/Dual Opteron 64 ou supérieur
- RAM : selon le modèle (4 Go ou supérieur)

- Espace disque : selon le modèle (250 Go ou supérieur)
- ESXi 5.0 ou ultérieur
- Configuration standard ou légère : vous devez choisir la configuration requise pour le disque dur de votre serveur. La configuration requise minimale est de 250 Go, sauf si la capacité de la machine virtuelle achetée est supérieure. Consultez les spécifications de votre machine virtuelle.

La machine virtuelle ENMELM utilise de nombreuses fonctionnalités qui ont besoin de ressources en processeur et RAM. Si l'environnement ESXi partage les ressources processeur et RAM requises avec d'autres machines virtuelles, cela aura des conséquences sur les performances de la machine virtuelle ENMELM. Veillez à inclure les besoins en ressources processeur et RAM dans la configuration requise.

Inspection de l'emballage et de l'équipement

Avant d'installer votre équipement, vérifiez l'absence de dommages ou d'altération.

Procédure

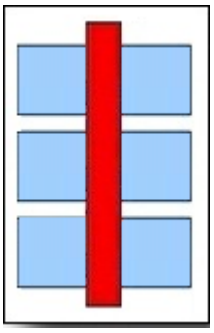
1 Dès que vous recevez votre équipement, inspectez-le ainsi que son emballage pour y rechercher des signes de dommages ou de mauvaise manipulation.

> Si vous procédez à une installation FIPS, inspectez le ruban d'emballage à bague d'inviolabilité qui sécurise l'unité de transport. Si une altération est manifeste, contactez immédiatement le support technique McAfee pour connaître les instructions à suivre, et n'installez pas le produit.

2 Vérifiez que tous les éléments répertoriés sur le bon de livraison sont présents dans l'emballage.

3 Lors d'une installation en mode FIPS, recherchez le sceau d'inviolabilité dans l'emballage des accessoires du conteneur de transport. Appliquez le sceau de façon à ce qu'il bloque complètement les ports USB, afin qu'ils ne puissent pas être utilisés sans le retrait du sceau (voir le schéma 1).

Schéma 1 : Positionnement du troisième sceau d'inviolabilité.



Contactez immédiatement le support technique McAfee si l'inspection ne vous satisfait pas pleinement.

Identification d'un emplacement pour l'installation

Vous devez analyser votre réseau existant et identifier un emplacement sur le réseau et un emplacement physique pour votre équipement. Le choix de l'emplacement a un impact sur l'efficacité d'utilisation de vos équipements.

Pour choisir l'emplacement des équipements :

- Installez votre équipement ESM dans un emplacement réseau qui lui permette de gérer les équipements et d'être accessible pour tous les systèmes qui accèdent à l'ESM. Si la communication directe entre les équipements managés par l'ESM ou les systèmes exécutant ESM est impossible, configurez votre réseau de façon à acheminer le trafic réseau entre eux.
- Placez l'équipement Nitro IPS entre le côté approuvé et le côté non approuvé du réseau. Le côté approuvé est celui que vous souhaitez protéger tandis que le côté non approuvé est celui que vous souhaitez laisser sans protection. Par exemple, vous pouvez placer votre équipement Nitro IPS entre le pare-feu (côté non approuvé) et le commutateur (côté approuvé). Comme les configurations réseau varient considérablement, l'emplacement que vous choisissez dépend de vos exigences de sécurité et de votre environnement réseau.

  Cet équipement est destiné à être installé dans un emplacement à accès restreint.

- Les équipements Receiver et DEM doivent être accessibles aux équipements qu'ils surveillent. Si aucune communication directe n'est possible, vous devez configurer votre réseau pour qu'il permette le routage approprié du trafic réseau entre eux.

Connexion et démarrage des équipements

Après avoir inspecté l'équipement et identifié l'emplacement privilégié pour l'installation, exécutez les étapes décrites dans cette section pour l'installer.

Procédure

1 Montez l'équipement.

Pour protéger l'équipement et le câblage contre tout dommage accidentel ou toute déconnexion, montez l'équipement dans un rack (consultez l'Annexe *Installation du kit de rails AXXVRAIL*).

a Préparez un espace pour l'équipement à l'emplacement de montage.

b Montez l'équipement de façon sécurisée à l'emplacement que vous avez sélectionné.

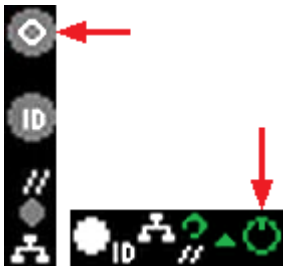
2 Connectez l'alimentation à l'équipement. Installez l'équipement et raccordez-le correctement à la terre conformément à ce manuel d'instructions et aux codes du pays, de l'Etat et de la localité.

Il est vivement conseillé de connecter tous les équipements ESM à un onduleur. Un système pourvu de cordons d'alimentation et de modules d'alimentation redondants fonctionnant dans des conditions normales équilibre le partage de charge grâce à sa conception parallèle, ce qui permet d'avoir un système d'alimentation fiable. Comme l'équipement Nitro IPS est en ligne, il doit être connecté à un onduleur.

3 Démarrez l'équipement.

a Procédez au câblage (le système doit être hors tension) et assurez-vous que le trafic est transmis.

b Activez l'équipement.



4 Sélectionnez le câble réseau.

5 Connectez les câbles aux ports approuvés et non approuvés. Si vous connectez des câbles à fibres optiques, retirez les enveloppes de protection des câbles et des connecteurs réseau uniquement lorsque vous êtes prêt à les connecter.

6 Vérifiez la connectivité de l'équipement en émettant une requête ping depuis le côté approuvé de votre réseau vers une adresse IP valide du côté non approuvé.

Voir aussi

Identification des types de connecteur et d'équipement, page 12
Identification des câbles réseau, page 12
Identification des ports réseau, page 13

Identification des types de connecteur et d'équipement

Vous pouvez connecter votre équipement Nitro IPS au réseau à l'aide de connecteurs en cuivre ou de fibres optiques en fonction du modèle de votre équipement.

Tableau 2-1 Type de connexion par équipement

Modèle Nitro IPS	Type de connecteur
TX	RJ-45 (cuivre)
SX	LC-Multimode (fibre optique)
LX	LC-Monomode (fibre optique)

Connectez vos équipements ESM, Receiver et DEM au réseau à l'aide des connecteurs en cuivre et identifiez les câbles en cuivre ou à fibres optiques en regardant les connecteurs. Le câble en cuivre CAT5 est pourvu de connecteurs RJ-45 (1) tandis que le câble à fibres optiques LC utilise des connecteurs de fibres optiques (2).

Il est conseillé d'utiliser des câbles CAT5 ou supérieurs pour votre connexion en cuivre. Pour une connexion Gigabit, il est conseillé d'utiliser des câbles CAT5e.

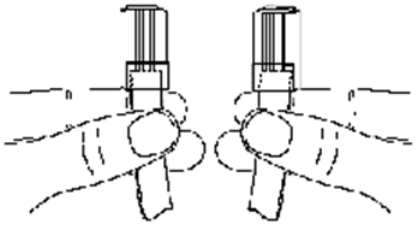
Type d'équipement

Vous pouvez connecter vos équipements ESM à deux types d'équipement : DCE (Data Circuit-Terminating Equipment) et DTE (Data Terminal Equipment). Le pare-feu, les routeurs et les équipements ESM sont de type DTE alors que les commutateurs sont de type DCE.

Identification des câbles réseau

Si votre équipement utilise une connexion par fibres optiques, vous devez sélectionner les câbles à fibres optiques et les connecter aux ports. Si votre équipement utilise une connexion en cuivre, utilisez un câble en cuivre droit ou croisé.

Pour connecter le port RJ-45 d'un équipement ESM à un équipement DCE, utilisez un câble droit. Pour le connecter à un équipement DTE, utilisez un câble croisé. Pour distinguer un câble droit d'un câble croisé, tenez les deux extrémités du câble comme indiqué ci-dessous :



Les fils de couleur d'un câble droit ont la même séquence aux deux extrémités. Dans un câble croisé, le premier (extrême gauche) fil de couleur à une extrémité est de la même couleur que le troisième fil de l'autre extrémité du câble.

Identification des ports réseau

Après avoir identifié les câbles dont vous avez besoin pour votre réseau, identifiez les ports de l'équipement McAfee auxquels vous allez connecter ces câbles.

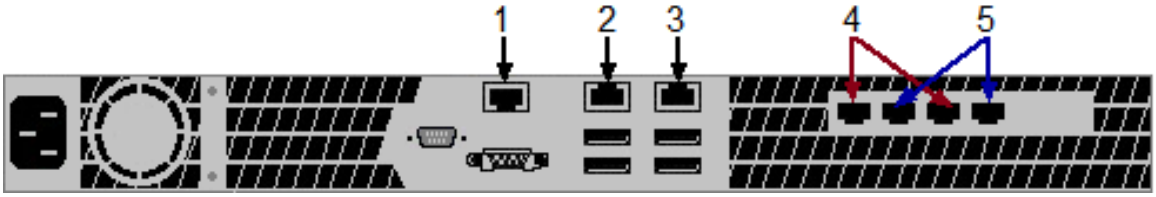
Désactivez toujours les éventuelles sources laser avant d'inspecter les connecteurs de fibres optiques, les composants optiques ou les partitions. Un rayonnement laser des fibres optiques peut être émis depuis les câbles à fibres optiques connectés ou les connecteurs de fibres optiques. Ne regardez pas directement dans l'équipement à fibres optiques. Conservez toujours un capuchon protecteur sur les connecteurs de fibres optiques non branchés.

Les équipements contiennent des ports de gestion afin de pouvoir être gérés depuis McAfee ESM. Par ailleurs, les équipements Nitro IPS et ADM contiennent des ports approuvés et non approuvés à connecter aux côtés approuvés et non approuvés du réseau.

Le tableau ci-dessous vous permet d'identifier les ports de gestion et les ports approuvés et non approuvés de l'ensemble de vos équipements.

Type d'équipement	Numéro de modèle	Chiffre
ACE	ACE-2600 ou 3450	2-8
ADM	APM-1250, 1260	2-1
	APM-3450, 3460	2-3
DEM	DSM-2600 ou 3450	2-3
	DSM-4600	2-4
ELM	ELM-4600, 5600 ou 6000	2-8
ELM/Récepteur	ELMERC-2600, 3450 ou 4600	2-8
ESM/ELM	ENMELM-4600, 5600 ou 6000	2-8
ESM ou combiné ESM/Récepteur	ETM-5600, 6000, X4 ou X6	2-8
	DAS-10, 25, 50 ou 100	2-9
IPS	NTP-1250	2-2
	NTP-2600, 3450-4BTX	2-3
	NTP-2600, 3450-8BTX	2-4
	NTP-2600, 3450-4BSX	2-5

Type d'équipement	Numéro de modèle	Chiffre
	NTP-3450-2BSX	2-6
McAfee Content Security Reporter	ERU-5600	2-8
Récepteur	ERC-1250,1260	2-2
	ERC-2600, 3450 ou 4600	2-7
Récepteur haute disponibilité	1U HA - ERC-1250-HA, 1260-HA	2-10, 2-11
	2U HA - ERC-2600 or 4600-HA	2-12, 2-13



1 IPMI

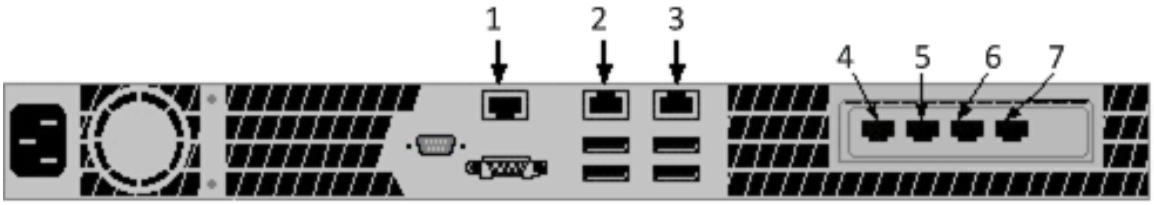
2 Gestion 2

3 Gestion 1

4 Approuvé

5 Non approuvé

Figure 2-1 NTP-1250



1 IPMI

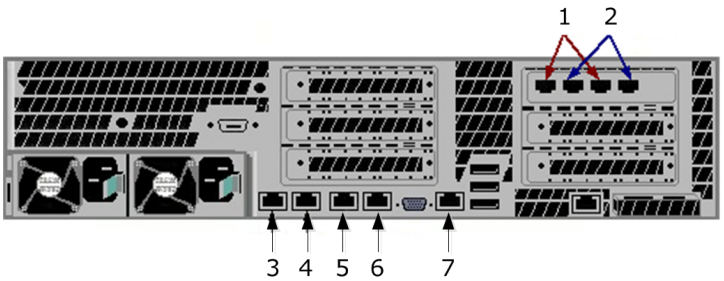
2 Gestion 2

3 Gestion 1

Pour les équipements APM-1250 et 1260, les ports 4 à 7 sont des ports de collecte (analyseur) et non des ports de gestion.

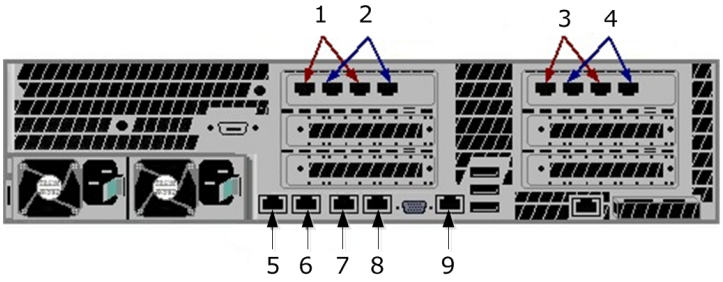
Pour les équipements ERC-1250, les ports 4 à 7 sont des ports de gestion supplémentaires.

Figure 2-2 ERC-1250, APM-1250, 1260



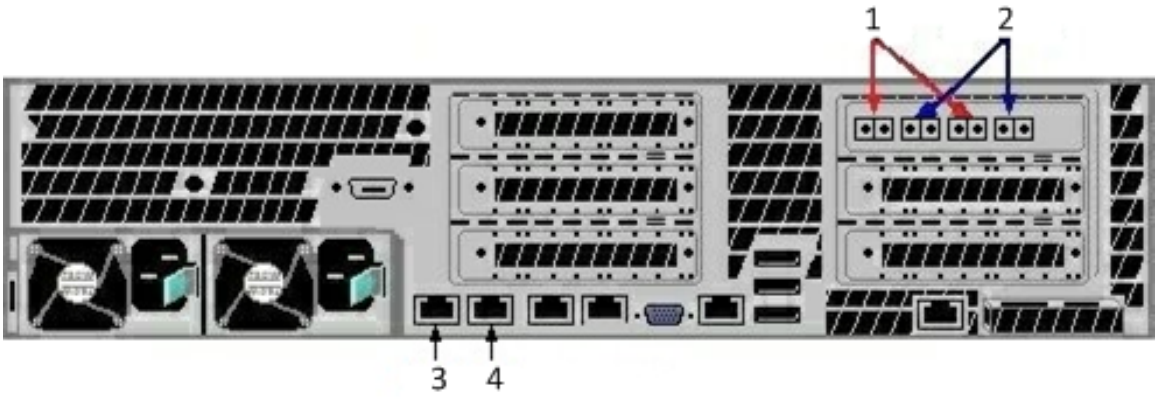
1 Approuvé
2 Non approuvé
3 Gestion 1
4 Gestion 2
5 Non utilisé
6 Non utilisé
7 Non utilisé

Figure 2-3 NTP-2600/3450-4BTX, 3460



1 Approuvé
2 Non approuvé
3 Approuvé
4 Non approuvé
5 Gestion 1
6 Gestion 2
7 Non utilisé
8 Non utilisé
9 Non utilisé

Figure 2-4 NTP-2600/3450-8BTX, DSM-4600

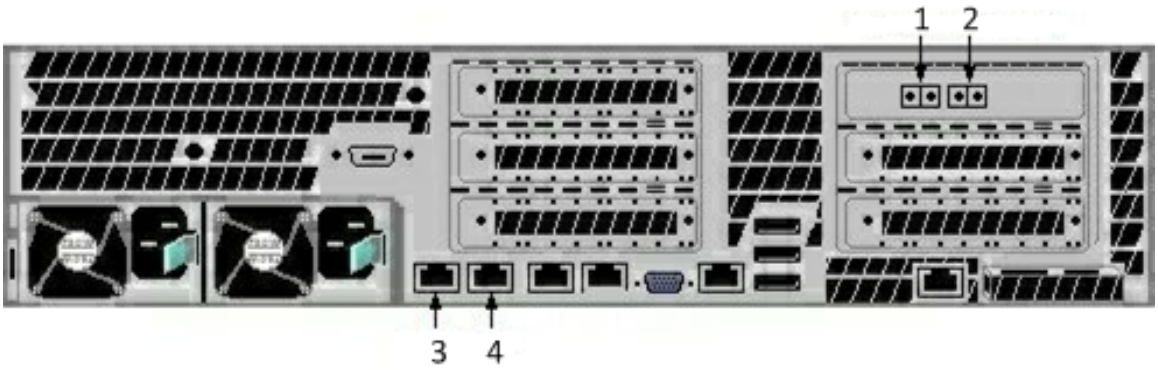


1 Approuvé
2 Non approuvé

3 Gestion 1

4 Gestion 2

Figure 2-5 NTP-2600/3450-4BSX



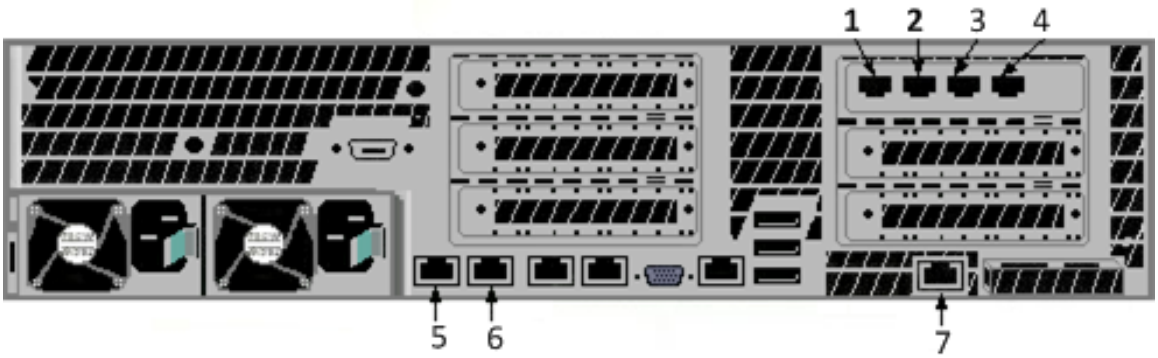
1 Approuvé

2 Non approuvé

3 Gestion 1

4 Gestion 2

Figure 2-6 NTP-3450-2BSX



1 IPMI NIC

2 Pulsations

5 Gestion

6 Données

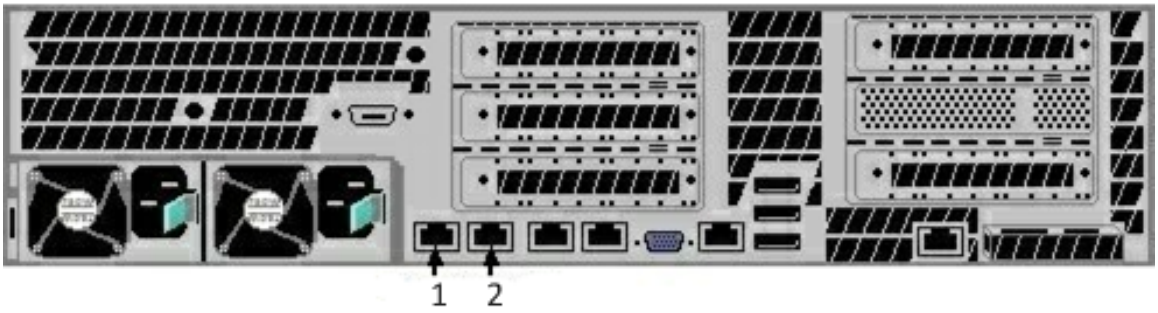
3 Gestion 2

4 Gestion 3

7 IPMI

Pour les équipements DSM-2600/3450 et APM-3450/3460, les ports 4 à 7 sont des ports de collecte (analyseur) et non des ports de gestion.

Figure 2-7 ERC-2600/3450/4600, DSM-2600/3450 et APM-3450/3460



1 Gestion 1

2 Gestion 2

Figure 2-8 ETM-5600/6000/X4/X6, ELMERC-2600/3450/4600, ELM-4600/5600/6000, ACE-2600/3450, ENMELM-4600/5600/6000, ERU-5600

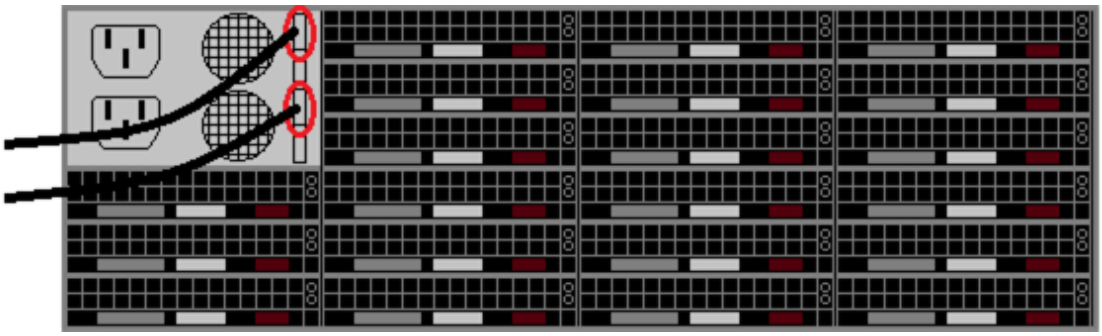
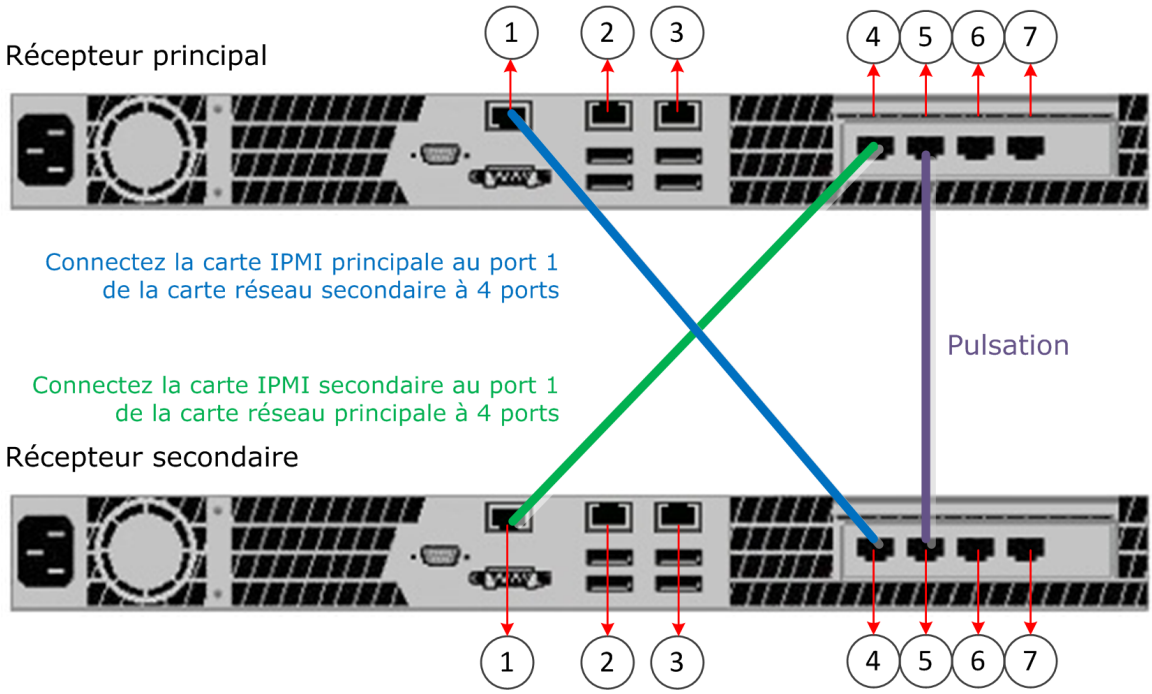
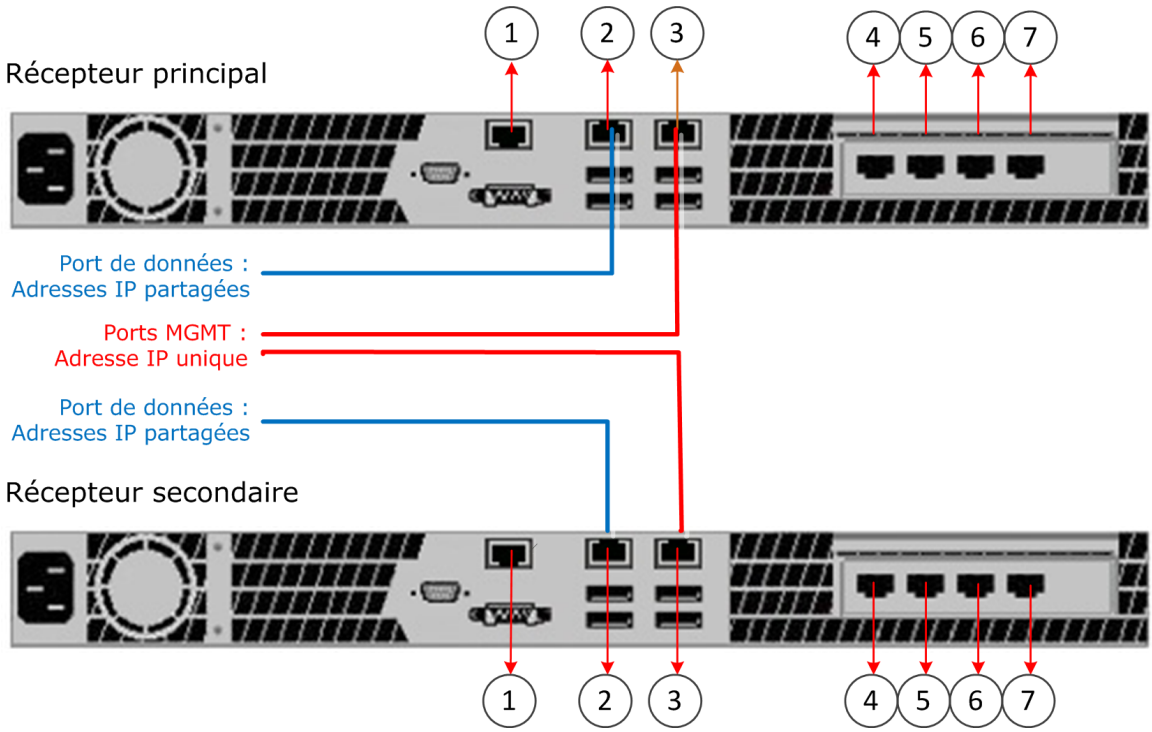


Figure 2-9 Câbles de données DAS



1	IPMI principale	4	IPMI secondaire
2	Gestion 2	5	Pulsation (HB)
3	Gestion 1	6	Gestion 3

Figure 2-10 Etape 1 : Créez la connexion entre les récepteurs 1U HA



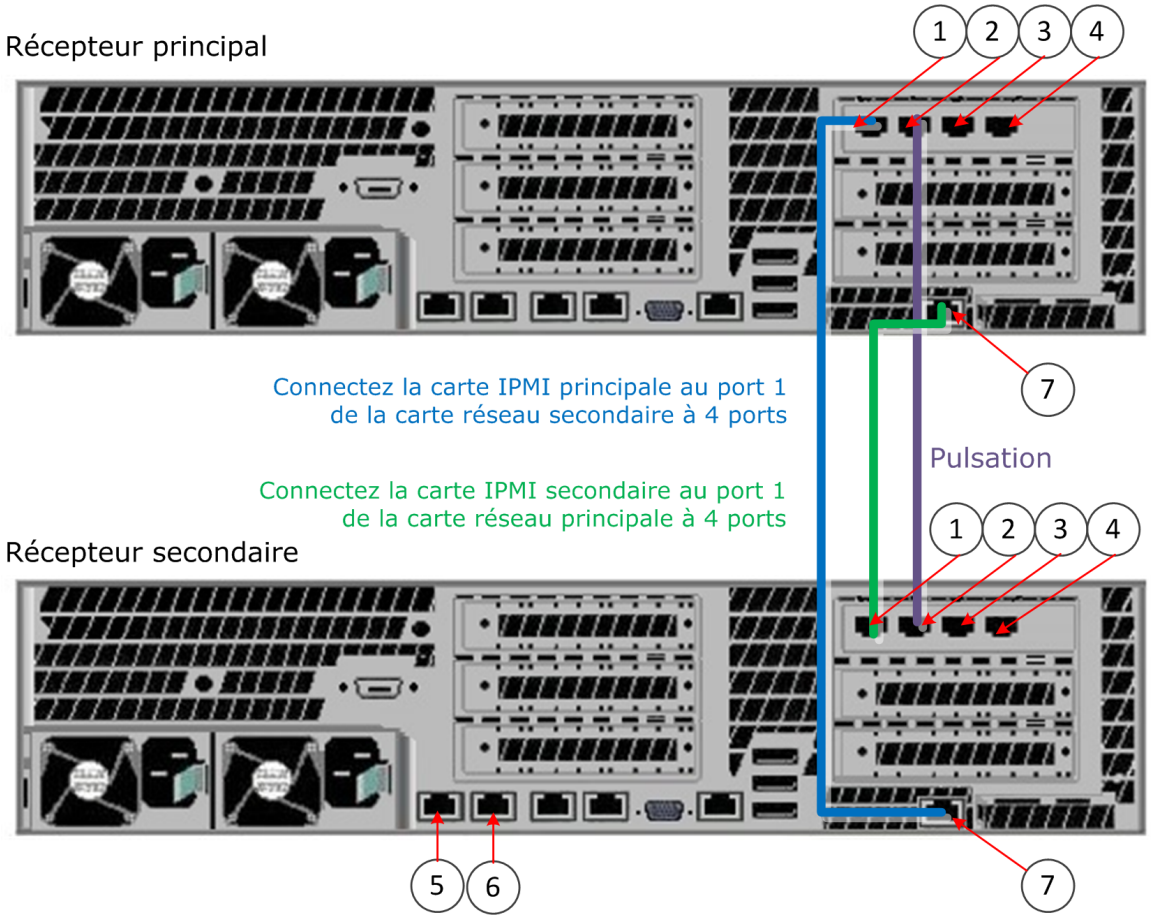
1	IPMI	5	Gestion 4 (eth3)
2	Gestion 2 (eth1)	6	Gestion 5 (eth4)

3 Gestion 1 (eth0)

4 Gestion 3 (eth2)

7 Gestion 6 (eth5)

Figure 2-11 Etape 2 : Connectez les récepteurs 1U HA au commutateur ou au routeur du réseau



1 IPMI

2 Gestion 2 (eth1)

5 Gestion 4 (eth3)

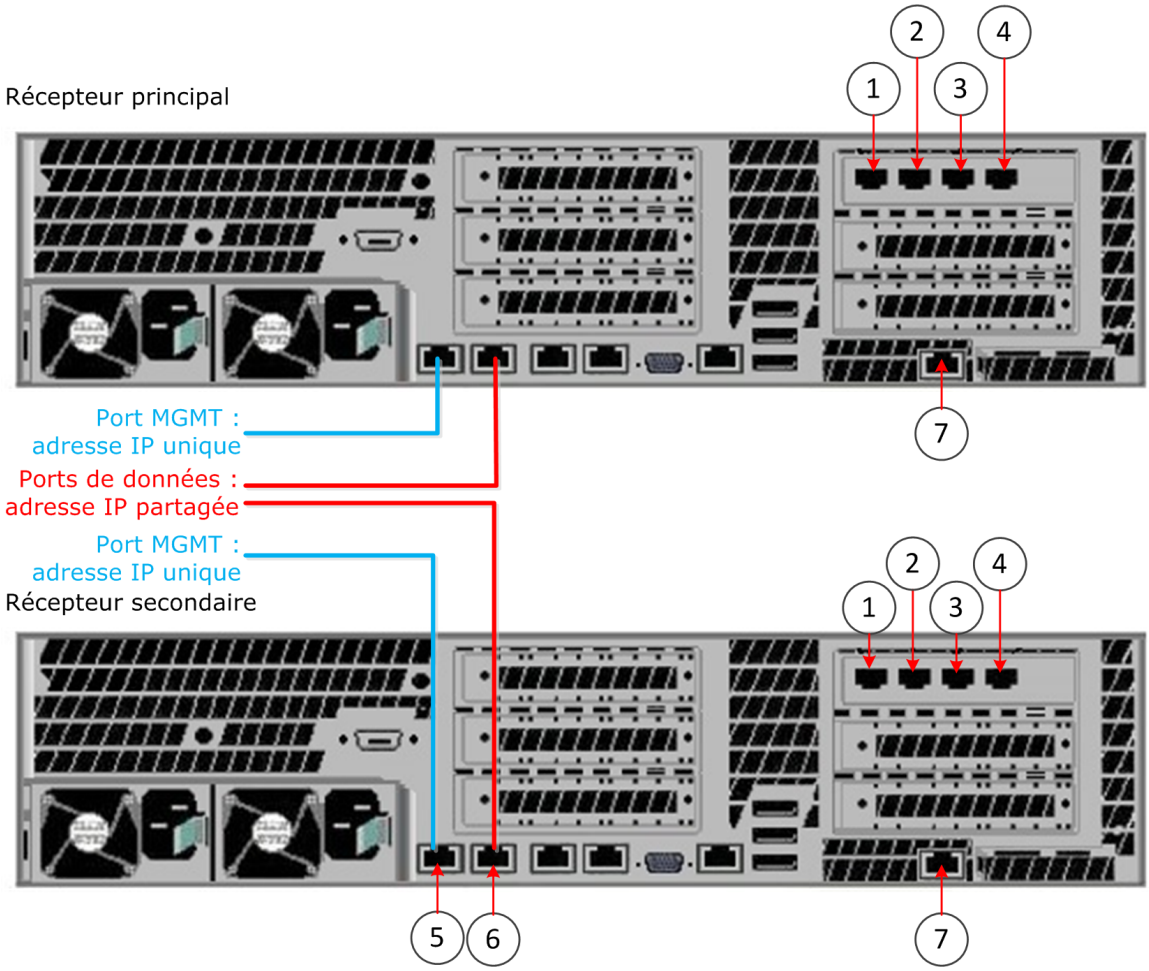
6 Gestion 5 (eth4)

3 Gestion 1 (eth0)

4 Gestion 3 (eth2)

7 Gestion 6 (eth5)

Figure 2-12 Etape 1 : Créez la connexion entre les récepteurs 2U HA



1 IPMI

2 Gestion 2 (eth1)

3 Gestion 1 (eth0)

4 Gestion 3 (eth2)

5 Gestion 4 (eth3)

6 Gestion 5 (eth4)

7 Gestion 6 (eth5)

Figure 2-13 Etape 2 : Connectez les récepteurs 2U HA au commutateur ou au routeur du réseau

Voir aussi

Identification d'un emplacement pour l'installation, page 10

3 Configuration des équipements McAfee ESM

La configuration des équipements est essentielle à leur bon fonctionnement. Pour les configurer, configurez IPv6 et l'interface réseau de chaque type d'équipement, puis connecter-vous à McAfee ESM.

Sommaire

- *Configuration de l'interface réseau dans Nitro IPS*
- *Configuration de l'interface réseau dans Receiver, ELM et ACE*
- *Configuration de l'interface réseau dans DEM et ADM*
- *Configuration de l'interface réseau dans ESM*
- *Configuration du protocole IPv6*
- *Connexion à la console McAfee ESM*

Configuration de l'interface réseau dans Nitro IPS

Suivez les étapes ci-dessous pour configurer les informations relatives à l'adresse IP.

Avant de commencer

Démarrez Nitro IPS et attendez la fin du processus de démarrage. Connectez un moniteur et un clavier à l'équipement.

Procédure

1. Appuyez sur **Alt + F1** pour accéder à la page LCD, puis appuyez deux fois sur **Echap**.
2. Faites défiler la page vers le bas jusqu'à l'option **MGT IP Conf** (Configuration d'IP de gestion), puis appuyez sur **Entrée**.
3. Sélectionnez **Mgt 1** (Gestion 1), puis appuyez sur **Entrée**.
4. Dans le menu **Active** (Actif), sélectionnez **IP Address** (Adresse IP), puis appuyez sur **Entrée**.
5. Définissez la valeur, puis appuyez sur **Entrée**.
6. Faites défiler la page vers le bas jusqu'à l'option **Netmask** (Masque réseau), puis définissez la valeur.
7. Faites défiler la page vers le bas jusqu'à l'option **Done** (Terminé), puis appuyez sur **Entrée**.
8. Faites défiler la page vers le bas jusqu'à l'option **Gateway** (Passerelle), puis appuyez sur **Entrée**.
9. Définissez l'adresse de la passerelle, faites défiler la page vers le bas jusqu'à l'option **Done** (Terminé), puis appuyez sur **Entrée**.

10 Faites défiler la page vers le bas jusqu'à l'option **Port Number** (Numéro de port), définissez la valeur, puis appuyez sur **Entrée**.

Notez le nouveau numéro de port, pour le saisir ensuite lors de l'activation de la clé sur l'équipement. Si le système fonctionne en mode FIPS, ne modifiez pas le numéro de port de communication.

11 Faites défiler la page vers le bas jusqu'à l'option **Save Changes** (Enregistrer les modifications), puis appuyez sur **Entrée**.

Configuration de l'interface réseau dans Receiver, ELM et ACE

Suivez les étapes ci-dessous pour configurer l'interface réseau sur un équipement Receiver, ELM ou ACE.

Avant de commencer
Connectez un moniteur et un clavier à l'équipement.

Procédure

1 Appuyez sur **Alt + F1** pour accéder à la page LCD, appuyez deux fois sur **Echap**, puis faites défiler la page vers le bas jusqu'à l'option **MGT IP Conf** (Configuration d'IP de gestion) et appuyez sur **Entrée**.

2 Sélectionnez **Mgt 1** (Gestion 1) et appuyez sur **Entrée**, puis sélectionnez **IP Address** (Adresse IP) et appuyez sur **Entrée**.

3 Définissez la valeur, puis appuyez sur **Entrée**.

4 Faites défiler la page vers le bas jusqu'à l'option **Netmask** (Masque réseau), puis définissez la valeur.

5 Faites défiler la page vers le bas jusqu'à l'option **Done** (Terminé), puis appuyez sur **Entrée**.

6 Faites défiler la page vers le bas jusqu'à l'option **Gateway** (Passerelle), puis appuyez sur **Entrée**.

7 Définissez l'adresse de la passerelle, faites défiler la page vers le bas jusqu'à l'option **Done** (Terminé), puis appuyez sur **Entrée**.

8 Faites défiler la page vers le bas jusqu'à l'option **DNS 1**, appuyez sur **Entrée**, puis définissez la valeur.

9 Faites défiler la page vers le bas jusqu'à l'option **Done** (Terminé), puis appuyez sur **Entrée**.

10 Si le mode FIPS est défini, faites défiler la page vers le bas jusqu'à l'option **Port Number** (Numéro de port), modifiez la valeur au besoin, puis appuyez sur **Entrée**.

Notez le nouveau numéro de port. Vous devrez le saisir lors de l'activation de la clé de l'équipement. Ne modifiez pas le port de communication TCP.

11 Faites défiler la page vers le bas jusqu'à l'option **Save Changes** (Enregistrer les modifications), puis appuyez sur **Entrée**.

Configuration de l'interface réseau dans DEM et ADM

Suivez les étapes ci-dessous pour configurer l'interface réseau dans un équipement DEM ou ADM.

Avant de commencer
Connectez un moniteur et un clavier à l'équipement.

Procédure

1 Appuyez sur **Alt + F1** pour accéder à la page LCD, puis appuyez deux fois sur **Echap**.

2 Faites défiler la page vers le bas jusqu'à l'option **MGT IP Conf** (Configuration d'IP de gestion), puis appuyez sur **Entrée**.

3 Sélectionnez **Mgt 1** (Gestion 1), puis appuyez sur **Entrée**.

4 Dans le menu **Active** (Actif), sélectionnez **IP Address** (Adresse IP), puis appuyez sur **Entrée**.

5 Définissez la valeur, puis appuyez sur **Entrée**.

6 Faites défiler la page vers le bas jusqu'à l'option **Netmask** (Masque réseau), puis définissez la valeur.

7 Faites défiler la page vers le bas jusqu'à l'option **Done** (Terminé), puis appuyez sur **Entrée**.

8 Faites défiler la page vers le bas jusqu'à l'option **Gateway** (Passerelle), puis appuyez sur **Entrée**.

9 Définissez l'adresse de la passerelle, faites défiler la page vers le bas jusqu'à l'option **Done** (Terminé), puis appuyez sur **Entrée**.

10 Si le mode FIPS est défini, faites défiler la page vers le bas jusqu'à l'option **Port Number** (Numéro de port), modifiez la valeur au besoin, puis appuyez sur **Entrée**.

Notez le nouveau numéro de port, pour le saisir ensuite lors de l'activation de la clé sur l'équipement. Ne modifiez pas le port de communication TCP.

11 Faites défiler la page vers le bas jusqu'à l'option **Save Changes** (Enregistrer les modifications), puis appuyez sur **Entrée**.

Configuration de l'interface réseau dans ESM

Suivez les étapes ci-dessous pour configurer l'interface réseau dans un ESM.

Avant de commencer

Activez ESM et vérifiez que le processus de redémarrage est terminé, puis connectez un moniteur et un clavier à l'équipement.

Procédure

1 Appuyez sur **Alt + F1** pour accéder à la page LCD, appuyez deux fois sur **Echap**, puis faites défiler la page vers le bas jusqu'à l'option **MGT IP Conf** (Configuration d'IP de gestion) et appuyez sur **Entrée**.

2 Sélectionnez **Mgt 1** (Gestion 1) et appuyez sur **Entrée**, puis sélectionnez **IP Address** (Adresse IP) et appuyez sur **Entrée**.

3 Définissez la valeur, puis appuyez sur **Entrée**.

4 Faites défiler la page vers le bas jusqu'à l'option **Netmask** (Masque réseau), puis définissez la valeur.

5 Faites défiler la page vers le bas jusqu'à l'option **Done** (Terminé), puis appuyez sur **Entrée**.

6 Faites défiler la page vers le bas jusqu'à l'option **Gateway** (Passerelle), puis appuyez sur **Entrée**.

7 Définissez l'adresse de la passerelle, faites défiler la page vers le bas jusqu'à l'option **Done** (Terminé), puis appuyez sur **Entrée**.

8 Faites défiler la page vers le bas jusqu'à l'option **DNS 1**, appuyez sur **Entrée**, puis définissez la valeur.

9 Faites défiler la page vers le bas jusqu'à l'option **Done** (Terminé), puis appuyez sur **Entrée**.

10 Faites défiler la page vers le bas jusqu'à l'option **Save Changes** (Enregistrer les modifications), puis appuyez sur **Entrée**.

Configuration du protocole IPv6

Si vous souhaitez utiliser le protocole IPv6 sur l'un de vos équipements et si votre réseau prend en charge la configuration automatique d'IPv6 sans état, configurez votre système pour qu'il gère IPv6.

Avant de commencer

Connectez un moniteur et un clavier à l'équipement.

Pour configurer manuellement une adresse pour ESM, consultez la section *Configuration des paramètres réseau* du *Guide Produit de McAfee Enterprise Security Manager*. Pour configurer manuellement une adresse pour chaque type d'équipement, consultez la section *Configuration des équipements* correspondant à l'équipement spécifique.

Procédure

1 Appuyez sur **Alt + F1** pour accéder à la page **LCD**, puis appuyez deux fois sur **Echap**.

2 Faites défiler la page vers le bas jusqu'à l'option **Configuration d'IPv6**, puis appuyez sur **Entrée**.

3 Sélectionnez **Mgt 1** (Gestion 1), puis appuyez sur **Entrée**.

4 Faites défiler la page vers le bas jusqu'à l'option **Enregistrer**, puis appuyez sur **Entrée**.

5 Pour localiser l'adresse IPv6 configurée automatiquement :

a Démarrez l'équipement et attendez le chargement du menu.

b Faites défiler la page vers le bas jusqu'à l'option **MGT IP Conf** (Configuration d'IP de gestion), puis appuyez sur **Entrée**.

c Faites défiler la page vers le bas jusqu'à l'option **Ipv6 Global** (IPv6 globale), puis appuyez sur **Entrée**.

d Vérifiez l'adresse IPv6, puis appuyez sur **Entrée** pour retourner dans le menu.

e Faites défiler la page vers le bas jusqu'à l'option **Done** (Terminé), puis appuyez sur **Entrée**.

f Faites défiler la page vers le bas jusqu'à l'option **Cancel Changes** (Annuler les modifications), puis appuyez sur **Entrée**.

Connexion à la console McAfee ESM

Lorsque vous avez installé et configuré ESM et les équipements, vous pouvez vous connecter à la console pour configurer les paramètres du système et des équipements.

Avant de commencer

Déterminez si vous devez utiliser le système en mode FIPS (consultez l'étape 5).

Procédure

1 Ouvrez un navigateur web sur votre ordinateur client et accédez à l'adresse IP que vous avez définie lorsque vous avez configuré l'interface réseau.

2 Cliquez sur **Connexion**, sélectionnez la langue de la console, puis entrez le nom d'utilisateur et le mot de passe par défaut.

- Nom de l'utilisateur par défaut : `NGCP`
- Mot de passe par défaut : `security.4u`

3 Cliquez sur **Connexion**, lisez l'**accord de licence utilisateur final**, puis cliquez sur **Accepter**.

4 A l'invite, modifiez vos nom d'utilisateur et mot de passe, puis cliquez sur **OK**.

5 Indiquez si vous souhaitez activer le mode FIPS.

Si vous devez utiliser le mode FIPS, vous devez l'activer lors de votre première connexion au système afin que toutes les futures communications avec les équipements McAfee soient en mode FIPS. N'activez pas le mode FIPS si vous n'avez pas l'obligation de l'utiliser. Pour plus d'informations sur le mode FIPS, consultez l'*Annexe A*.

6 Suivez les instructions affichées pour obtenir vos nom d'utilisateur et mot de passe, qui sont nécessaires pour accéder aux mises à jour des règles.

7 Effectuez la configuration initiale de l'ESM :

a Sélectionnez la langue à utiliser pour les journaux système.

b Sélectionnez le fuseau horaire correspondant à cet ESM ainsi que le format de date à utiliser avec ce compte, puis cliquez sur **Suivant**.

c Définissez les paramètres dans les cinq pages de l'Assistant **Configuration ESM initiale** en cliquant sur l'icône **Aide** de chaque page pour obtenir les instructions.

8 Cliquez sur **OK**.

Vous êtes prêt à activer la clé des équipements et à configurer ces derniers. Voir le *Guide Produit de McAfee Enterprise Security Manager*.

A A propos du mode FIPS

La norme FIPS (Federal Information Processing Standard) est constituée de normes annoncées publiquement, qui sont développées par le gouvernement fédéral des Etats-Unis. Si vous devez respecter ces normes, vous devez utiliser ce système en mode FIPS.

Le mode FIPS doit être sélectionné la première fois que vous vous connectez au système et il ne peut pas être modifié par la suite.

Sommaire

- *Informations sur le mode FIPS*
- *Sélection du mode FIPS*
- *Vérification de l'intégrité FIPS*
- *Ajout d'un équipement dont la clé est activée en mode FIPS*
- *Résolution des problèmes liés au mode FIPS*

Informations sur le mode FIPS

En raison de la réglementation FIPS, certaines fonctionnalités ESM ne sont pas disponibles, certaines fonctionnalités disponibles ne sont pas conformes et d'autres fonctionnalités ne sont disponibles qu'en mode FIPS. Ces fonctionnalités sont notées tout au long du document et répertoriées ici.

Statut de la fonctionnalité	Description
Fonctionnalités supprimées	• Récepteurs haute disponibilité. • Terminal GUI (interface graphique utilisateur). • Communication avec l'équipement qui utilise le protocole SSH. • Dans la console de l'équipement, le shell racine est remplacé par un menu de gestion des équipements.
Fonctionnalités disponibles uniquement en mode FIPS	• Il existe quatre rôles d'utilisateur qui ne se chevauchent pas : **Utilisateur**, **Utilisateur avec pouvoir**, **Administrateur d'audit** et **Administrateur de clé et certificat**. • Toutes les pages **Propriétés** sont pourvues de l'option **Auto-test** qui vous permet de vérifier que le système fonctionne correctement en mode FIPS. • En cas d'échec FIPS, un indicateur de statut est ajouté à l'arborescence de navigation des systèmes pour refléter cet échec. • Toutes les pages **Propriétés** sont pourvues de l'option **Afficher**, qui ouvre la page **Jeton d'identité FIPS** lorsque vous cliquez dessus. Elle affiche une valeur qui doit être comparée à la valeur affichée dans ces sections du document afin que vous vous assuriez que le mode FIPS n'a pas été compromis. • Dans **Propriétés du système** | **Utilisateurs et groupes** | **Privilèges** | **Modifier le groupe**, la page inclut le privilège **Auto-test du chiffrement FIPS**, qui octroie aux membres de groupe l'autorisation d'exécuter des auto-tests FIPS. • Lorsque vous cliquez sur **Importer la clé** ou **Exporter la clé** dans **Propriétés IPS** | **Gestion des clés**, vous êtes invité à sélectionner le type de clé que vous souhaitez importer ou exporter. • Dans l'**Assistant Ajout d'équipement**, le protocole TCP est toujours défini sur le port 22. Le port SSH peut être modifié.

Sélection du mode FIPS

Lors de la première connexion au système, vous devez décider si le système doit fonctionner en mode FIPS ou non. Une fois cette sélection effectuée, il n'est pas possible de la modifier.

Procédure

Pour consulter la définition des options, cliquez sur **?** dans l'interface.

1 Lors de votre première connexion à ESM :

   a Dans le champ **Nom de l'utilisateur**, entrez `NGCP`.

   b Dans le champ **Mot de passe**, entrez `security.4u`.

   Vous êtes invité à changer votre mot de passe.

2 Entrez et confirmez le nouveau mot de passe.

3 Dans **Activer FIPS**, cliquez sur **Oui**.

Le message d'avertissement **Activer FIPS** vous demande de confirmer que vous souhaitez faire fonctionner ce système en mode FIPS de façon définitive.

4 Cliquez sur **Oui** pour confirmer votre choix.

Vérification de l'intégrité FIPS

Si votre système fonctionne en mode FIPS, FIPS 140-2 requiert la vérification régulière de l'intégrité logicielle. Cette vérification doit être effectuée sur le système et sur chaque équipement.

Procédure

Pour consulter la définition des options, cliquez sur **?** dans l'interface.

1 Dans l'arborescence de navigation des systèmes, sélectionnez **Propriétés du système** et assurez-vous que l'option **Informations système** est sélectionnée.

2 Effectuez l'une des actions suivantes :

Dans ce champ...	Procédez ainsi...
Statut FIPS	Afficher les résultats du dernier auto-test FIPS effectué sur l'ESM.
Test ou **Auto-test FIPS**	Exécuter les auto-tests FIPS qui permettent de vérifier l'intégrité des algorithmes utilisés dans l'exécutable de chiffrement. Vous pouvez consulter les résultats dans le **Journal des messages**. Si un auto-test FIPS échoue, FIPS est compromis ou une défaillance de l'équipement s'est produite. Contactez le Support technique McAfee.
Afficher ou **Identité FIPS**	Ouvrez la page **Jeton d'identité FIPS** pour exécuter la vérification de l'intégrité logicielle au démarrage. Comparez la valeur ci-dessous à la clé publique qui s'affiche sur cette page : -----BEGIN PUBLIC KEY----- MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAt8FWOP2mvVjvTTxkhGqk LdgA+sx0jBv+zYnCkGYOHHzNAdum9yuMn69GNbYXm7I5OcKv2+nz6axBruCZ5XX1 jCGWnmsj8YZJoNp/FLUy1jYE7lXI5/NRm2uhjhzjdOjgFv10SkgxVfL/aBJjqZFJ KKbHMzYEBwdyseQUc56u3mKaBtP4rydfRmEtytkuOsZgQuPHKYhaQJlnbV5LfrLa o6HQSlzHYHlcF/Yog+QHJ6ClSRA1lk8MPyFG9RHdKnwcq3sY8QjQMbIZ5SDobbK0 GPOOucG8vWDWdxSiabJLBdklVsmB0zwdH6lOCkkGTidayMk12hDh+2BA6el7YQBV 8EJaJ5wvz8aQKwDfiinlb9vmC+sk+Rwo/E7uRn3El4+RxouHi9J3f92I9qXZeJCV iYV2XahhyxSpq8ro/j0BMTiab3dIjjogxMxCI9QjEpm3J/ZyUpWtNKaHq8BgSE1e daiJob7O/kvef1T/ZOb3O90bSK3vtn+3Si3K3cpaY/qBm9var6xVNyGhHztRJv0F 0nSJlyddWuXL1U+hMTO2YE33T3s4Uf4jiomTVSDTJ087hLT5l/hCz6A33Hzl7gk8 Q89SNsmL/p0RAJzJ3+mGyoUAd1D2u6sYq6NkGCn640a5A2zAOQdX/M8R8S+NKjgi nLg3n+/+25KsCB3KDY3AkYECAwEAAQ== -----END PUBLIC KEY----- Si cette valeur ne correspond pas à la clé publique, FIPS est compromis. Contactez le Support technique McAfee.

Ajout d'un équipement dont la clé est activée en mode FIPS

En mode FIPS, deux méthodes permettent d'ajouter à un ESM un équipement dont la clé a déjà été activée. Cette terminologie ainsi que les extensions de fichier vous sont utiles lorsque vous suivez ces procédures.

Terminologie

- **Clé d'équipement** : contient les droits de gestion dont dispose un ESM pour un équipement. Elle n'est pas utilisée pour la cryptographie.
- **Clé publique** : clé de communication SSH publique d'ESM, qui est stockée dans la table des clés autorisées d'un équipement.
- **Clé privée** : clé de communication SSH privée d'ESM, qui est utilisée par l'exécutable SSH dans un ESM pour établir la connexion SSH avec un équipement.
- **ESM principal** : ESM qui a été utilisé à l'origine pour enregistrer l'équipement.
- **ESM secondaire** : ESM supplémentaire qui communique avec l'équipement.

Extensions des différents fichiers d'exportation

- **.exk** : contient la clé d'équipement.
- **.puk** : contient la clé publique.
- **.prk** : contient la clé privée et la clé d'équipement.

Sauvegarde et restauration des informations d'un équipement en mode FIPS

Cette méthode permet de sauvegarder et de restaurer les informations de communication d'un équipement sur l'ESM.

Elle est principalement destinée à être utilisée en cas de défaillance nécessitant le remplacement d'ESM. Si les informations de communication ne sont pas exportées avant la défaillance, il est impossible de rétablir la communication avec l'équipement. Cette méthode exporte et importe le fichier .prk.

La clé privée de l'ESM principal est utilisée par l'ESM secondaire pour établir initialement une communication avec l'équipement. Une fois la communication établie, l'ESM secondaire copie sa clé publique dans la table des clés autorisées de l'équipement. L'ESM secondaire efface alors la clé privée de l'ESM principal et initie une communication avec sa propre paire de clés publiques ou privées.

Action	Etapes
Exporter le fichier .prk à partir de l'ESM principal	1 Dans l'arborescence de navigation des systèmes de l'ESM principal, sélectionnez l'équipement pourvu des informations de communication que vous souhaitez sauvegarder, puis cliquez sur l'icône **Propriétés**. 2 Sélectionnez **Gestion des clés**, puis cliquez sur **Exporter la clé**. 3 Sélectionnez **Sauvegarder la clé privée SSH**, puis cliquez sur **Suivant**. 4 Tapez et confirmez un mot de passe, puis définissez la date d'expiration. Une fois la date d'expiration passée, la personne qui importe la clé ne peut pas communiquer avec l'équipement tant qu'aucune autre clé n'a été exportée avec une date d'expiration future. Si vous sélectionnez **Ne jamais expirer**, la clé n'expire jamais si elle est importée dans un autre ESM. 5 Cliquez sur **OK**, sélectionnez l'emplacement d'enregistrement du fichier .prk créé par l'ESM, puis déconnectez-vous de l'ESM principal.
Ajouter un équipement à l'ESM secondaire et importer le fichier .prk	1 Dans l'arborescence de navigation des systèmes de l'équipement secondaire, sélectionnez le nœud de niveau Système ou Groupe auquel vous souhaitez ajouter l'équipement. 2 Dans la barre d'outils Actions, cliquez sur **Ajouter un équipement**. 3 Sélectionnez le type d'équipement à ajouter, puis cliquez sur **Suivant**. 4 Entrez le nom de l'équipement qui est unique dans ce groupe, puis cliquez sur **Suivant**. 5 Entrez l'adresse IP cible de l'équipement et le port de communication FIPS, puis cliquez sur **Suivant**. 6 Cliquez sur **Importer la clé**, sélectionnez le fichier .prk précédemment exporté, puis cliquez sur **Charger**. Tapez le mot de passe spécifié lors de l'exportation initiale de cette clé. 7 Déconnectez-vous de l'ESM secondaire.

Activation de la communication avec plusieurs équipements ESM en mode FIPS

Vous pouvez permettre à plusieurs ESM de communiquer avec le même équipement. Pour cela, exportez et importez les fichiers .puk et .exk.

Cette méthode utilise deux processus d'exportation et d'importation. L'ESM principal est d'abord utilisé pour importer le fichier .puk exporté depuis l'équipement ESM secondaire et envoyer la clé publique de l'ESM secondaire vers l'équipement. Cela permet aux deux équipements ESM de communiquer avec l'équipement. Ensuite, le fichier .exk de l'équipement est exporté depuis l'ESM principal et importé vers l'ESM secondaire, ce qui permet à l'ESM secondaire de communiquer avec l'équipement.

Action	Etapes
Exporter le fichier .puk à partir de l'ESM secondaire	1 Dans la page **Propriétés du système** de l'ESM secondaire, sélectionnez **Gestion ESM**. 2 Cliquez sur **Exporter SSH**, puis sélectionnez l'emplacement d'enregistrement du fichier .puk. 3 Cliquez sur **Enregistrer**, puis déconnectez-vous.
Importer le fichier .puk dans l'ESM principal	1 Dans l'arborescence de navigation des systèmes de l'ESM principal, sélectionnez l'équipement que vous souhaitez configurer. 2 Cliquez sur l'icône **Propriétés**, puis sélectionnez **Gestion des clés**. 3 Cliquez sur **Gérer les clés SSH**. 4 Cliquez sur **Importer**, sélectionnez le fichier .puk, puis cliquez sur **Charger**. 5 Cliquez sur **OK**, puis déconnectez-vous de l'ESM principal.
Exporter le fichier .exk de l'équipement à partir de l'ESM principal	1 Dans l'arborescence de navigation des systèmes de l'ESM principal, sélectionnez l'équipement que vous souhaitez configurer. 2 Cliquez sur l'icône **Propriétés**, puis sélectionnez **Gestion des clés**. 3 Cliquez sur **Exporter la clé**, sélectionnez la clé de l'équipement de sauvegarde, puis cliquez sur **Suivant**. 4 Tapez et confirmez un mot de passe, puis définissez la date d'expiration. Une fois la date d'expiration passée, la personne qui importe la clé ne peut pas communiquer avec l'équipement tant qu'aucune autre clé n'a été exportée avec une date d'expiration future. Si vous sélectionnez **Ne jamais expirer**, la clé n'expire jamais si elle est importée dans un autre ESM. 5 Sélectionnez les privilèges du fichier .exk, puis cliquez sur **OK**. 6 Sélectionnez l'emplacement d'enregistrement de ce fichier, puis déconnectez-vous de l'ESM principal.
Importer le fichier .exk dans l'ESM secondaire	1 Dans l'arborescence de navigation des systèmes de l'équipement secondaire, sélectionnez le nœud de niveau Système ou Groupe auquel vous souhaitez ajouter l'équipement. 2 Dans la barre d'outils Actions, cliquez sur **Ajouter un équipement**. 3 Sélectionnez le type d'équipement à ajouter, puis cliquez sur **Suivant**. 4 Entrez le nom de l'équipement propre à ce groupe, puis cliquez sur **Suivant**. 5 Cliquez sur **Importer la clé**, puis naviguez jusqu'au fichier .exk. 6 Cliquez sur **Charger**, puis entrez le mot de passe qui a été spécifié lors de l'exportation initiale de cette clé. 7 Déconnectez-vous de l'ESM secondaire.

Résolution des problèmes liés au mode FIPS

Des problèmes peuvent se produire lorsque ESM fonctionne en mode FIPS.

Problème	Description et résolution
Communication impossible avec l'ESM	• Consultez l'écran LCD à l'avant de l'équipement. Si un message indique un **Echec FIPS**, contactez le support technique McAfee. • Déterminez si l'interface HTTP présente une condition d'erreur en consultant la page web d'auto-test FIPS de l'ESM dans un navigateur. - Si le chiffre unique **0** s'affiche, indiquant l'échec de l'auto-test FIPS sur l'équipement, redémarrez l'équipement ESM pour essayer de corriger le problème. Si la condition d'échec persiste, contactez le support technique pour obtenir d'autres instructions. - Si le chiffre unique **1** s'affiche, le problème de communication n'est pas dû à un échec FIPS. Pour connaître la procédure de résolution, contactez le support technique.
Communication impossible avec l'équipement	• Si un indicateur d'état s'affiche à côté de l'équipement dans l'arborescence de navigation du système, placez le curseur dessus. Si le message **Echec FIPS** s'affiche, contactez le support technique McAfee via le portail de support. • Suivez les instructions relatives au problème *Communication impossible avec l'ESM*.
Erreur **Le fichier n'est pas valide** lors de l'ajout d'un équipement	Vous ne pouvez pas exporter une clé d'un équipement qui n'est pas en mode FIPS pour l'importer sur un équipement qui est en mode FIPS. De même, vous ne pouvez pas exporter une clé d'un équipement qui est en mode FIPS pour l'importer sur un équipement qui n'est pas en mode FIPS. Cette erreur s'affiche si vous essayez de faire ces opérations.

B Configuration requise pour une machine virtuelle ESXi

La machine virtuelle doit être conforme à la configuration minimale suivante.

- Processeur : 8 cœurs ou supérieur, selon le modèle, 64 bits, Dual Core 2/Nehalem ou supérieur ou AMD Dual Athlon 64/Dual Opteron 64 ou ultérieur
- RAM : selon le modèle (4 Go ou supérieur)
- Disque : selon le modèle (250 Go ou supérieur)
- ESXi : 5.0 ou ultérieur

Vous pouvez sélectionner la capacité requise du disque dur de votre serveur. Mais la capacité requise pour la machine virtuelle dépend du modèle de l'équipement (250 Go ou plus). Si vous ne disposez pas d'au moins 250 Go disponibles, un message d'erreur s'affiche lors du déploiement de la machine virtuelle.

La machine virtuelle utilise de nombreuses fonctionnalités qui requièrent des ressources en processeur et RAM. Si l'environnement ESXi partage les ressources processeur et RAM requises avec d'autres machines virtuelles, de quelque manière que ce soit, cela entraîne des conséquences sur les performances de la machine virtuelle. Planifiez les besoins en processeur et RAM en fonction de la configuration requise indiquée ici.

McAfeeIl est conseillé de choisir l'option de configuration **Thick** (Standard).

Sommaire

- *Modèles de machine virtuelle (VM)*
- *Agrégation par bandes du lecteur de stockage*
- *Installation de la machine virtuelle*
- *Configuration de la machine virtuelle*
- *Activation de la clé de l'équipement virtuel*

Modèles de machine virtuelle (VM)

Le tableau suivant répertorie les modèles de machine virtuelle disponibles, le nombre d'événements par seconde (EPS) que chaque modèle peut traiter, le stockage mécanique recommandé, la capacité

de stockage du lecteur SSD et les conditions requises pour la plateforme qui exécute la machine virtuelle.

Numéro de modèle	Capacité EPS	Stockage mécanique	SSD	Configuration requise pour la plateforme
ELU4 ELU12	1,000 5,000	Environnement de machine virtuelle recommandé de 250 Go Machine virtuelle recommandée Environnement de 500 Go minimum	Néant 240 Go minimum	VMware ESX/ESXi Server v. 5.x+, processeur 8 cœurs (processeur Intel® Xeon® E5 ou E7), mémoire de 4 Go VMware ESX/ESXi Server v. 5.x+, processeur 12 cœurs (processeur Intel® Xeon® E5 ou E7), mémoire de 64 Go
ENU4 ENU12 ENU32	1,500* 40,000* 85,000*	Environnement de machine virtuelle recommandé de 250 Go Environnement de machine virtuelle recommandé de 500 Go minimum Environnement de machine virtuelle recommandé de 2 To minimum	Néant 480 Go minimum 3 To minimum	VMware ESX/ESXi Server v. 5.x+, processeur 8 cœurs (processeur Intel® Xeon® E5 ou E7), mémoire de 4 Go VMware ESX/ESXi Server v. 5.x+, processeur 12 cœurs (processeur Intel® Xeon® E5 ou E7), mémoire de 64 Go VMware ESX/ESXi Server v. 5.x+, processeur 32 cœurs (processeur Intel® Xeon® E5 ou E7), mémoire de 96 Go
ELM4 ELM12 ELM32	1,500* 30,000* 70,000*	Environnement de machine virtuelle recommandé de 250 Go Environnement de machine virtuelle recommandé de 500 Go minimum Environnement de machine virtuelle recommandé de 2 To minimum	Néant 480 Go minimum 3 To minimum	VMware ESX/ESXi Server v. 5.x+, processeur 8 cœurs (processeur Intel® Xeon® E5 ou E7), mémoire de 4 Go VMware ESX/ESXi Server v. 5.x+, processeur 12 cœurs (processeur Intel® Xeon® E5 ou E7), mémoire de 64 Go VMware ESX/ESXi Server v. 5.x+, processeur 32 cœurs (processeur Intel® Xeon® E5 ou E7), mémoire de 96 Go
EV2 EV5 EV10	500 5,000 15,000	Environnement de machine virtuelle recommandé de 250 Go Environnement de machine virtuelle recommandé de 500 Go minimum Environnement de machine virtuelle recommandé de 2 To minimum	Néant 480 Go minimum 3 To minimum	VMware ESX/ESXi Server v. 5.x+, processeur 8 cœurs (processeur Intel® Xeon® E5 ou E7), mémoire de 4 Go VMware ESX/ESXi Server v. 5.x+, processeur 12 cœurs (processeur Intel® Xeon® E5 ou E7), mémoire de 64 Go VMware ESX/ESXi Server v. 5.x+, processeur 32 cœurs (processeur Intel® Xeon® E5 ou E7), mémoire de 96 Go

Numéro de modèle	Capacité EPS	Stockage mécanique	SSD	Configuration requise pour la plateforme
ELMERCVM4 ELMERCVM12	1,500 5,000	Environnement de machine virtuelle recommandé de 250 Go Environnement de machine virtuelle recommandé de 500 Go minimum	Néant 240 Go minimum	VMware ESX/ESXi Server v. 5.x+, processeur 8 cœurs (processeur Intel® Xeon® E5 ou E7), mémoire de 4 Go VMware ESX/ESXi Server v. 5.x+, processeur 12 cœurs (processeur Intel® Xeon® E5 ou E7), mémoire de 64 Go
ACV12 ACV32	<30,000* <80,000*	Environnement de machine virtuelle recommandé de 250 Go Environnement de machine virtuelle recommandé de 500 Go minimum	480 Go minimum 3 To minimum	VMware ESX/ESXi Server v. 5.x+, processeur 12 cœurs (processeur Intel® Xeon® E5 ou E7), mémoire de 64 Go VMware ESX/ESXi Server v. 5.x+, processeur 32 cœurs (processeur Intel® Xeon® E5 ou E7), mémoire de 96 Go
APM4 APM12	250 Mbits/s 500 Mbits/s	Environnement de machine virtuelle recommandé de 250 Go Environnement de machine virtuelle recommandé de 500 Go minimum	Néant 480 Go minimum	VMware ESX/ESXi Server v. 5.x+, processeur 8 cœurs (processeur Intel® Xeon® E5 ou E7), mémoire de 4 Go VMware ESX/ESXi Server v. 5.x+, processeur 12 cœurs (processeur Intel® Xeon® E5 ou E7), mémoire de 64 Go

Agrégation par bandes du lecteur de stockage

Si la capacité du modèle est supérieure à 250 Go et que le paramètre **256 MB to 2 MB** (256 Mo à 2 Go) est nécessaire, agrégez par bandes le lecteur de stockage de la machine virtuelle.

Procédure

1 Sélectionnez le serveur ESX, cliquez sur l'onglet **Configuration**, puis sur **Storage** (Stockage) dans la section **Hardware** (Matériel).

La machine virtuelle utilise de nombreuses fonctionnalités qui requièrent des ressources en processeur et RAM. Si l'environnement ESXi partage les ressources processeur et RAM requises avec d'autres machines virtuelles, cela aura des conséquences sur les performances de la machine virtuelle. Planifiez les besoins en processeur et RAM en fonction de la configuration requise.

2 Cliquez sur **Add Storage** (Ajouter du stockage), puis sélectionnez **Disk/LUN** (Disque/Numéro d'unité logique).

3 Sélectionnez un disque disponible, puis sélectionnez l'option appropriée à l'espace disque disponible. **Use 'Free space'** (Utiliser l'espace libre) s'il s'agit d'un lecteur existant ou **Use all available partitions** (Utiliser toutes les partitions disponibles) s'il s'agit d'un lecteur disponible.

Vous pouvez sélectionner la capacité requise du disque dur de votre serveur, mais la configuration requise pour la machine virtuelle est de 500 Go. Si vous ne disposez pas de 500 Go disponibles, un message d'erreur s'affiche lors du déploiement de la machine virtuelle. McAfeeIl est conseillé de choisir la configuration **Thick** (Standard).

4 Attribuez un nom au lecteur de stockage, puis sélectionnez **512 GB, Block size: 2 MB** (512 Go, taille des blocs : 2 Mo) dans la liste déroulante **Maximum file size** (Taille de fichier maximale) pour assurer un espace disponible de 500 Go.

Installation de la machine virtuelle

Une fois que vous avez installé une machine virtuelle et activé sa clé, elle reproduit le fonctionnement normal d'ESM.

Avant de commencer

Vérifiez que votre équipement satisfait à la configuration requise minimale.

Procédure

1 Accédez à la racine du lecteur de CD (dans le cas d'une installation à partir d'un CD) ou téléchargez sur l'ordinateur local les fichiers fournis par le support technique McAfee.

2 Dans **vSphere Client** (Client vSphere), cliquez sur l'adresse IP du serveur dans l'arborescence des équipements.

3 Cliquez sur **File** (Fichier), puis sélectionnez **Deploy OVF Template**(Déployer le modèle OVF).

4 Désignez le nom, le dossier d'installation de la machine virtuelle, le paramètre de configuration du disque et l'option **VM Networking** (Réseau de la machine virtuelle).

5 Déployez les fichiers sur le serveur ESXi, sélectionnez la machine virtuelle et assurez-vous que les éléments suivants sont définis dans le paramètre **Edit Virtual Machine** (Modifier la machine virtuelle).

6 Sélectionnez les paramètres réseau appropriés pour vos commutateurs/cartes réseau ESXi, puis cliquez sur **Play** (Lire) pour lancer la machine virtuelle.

7 Dans le menu VM, définissez l'adresse IP gestion 1, ainsi que l'adresse de masque réseau, de passerelle et DNS, puis appuyez sur **Echap** pour activer le menu.

8 Configurez l'interface réseau sur la machine virtuelle, enregistrez les modifications avant de quitter la fenêtre **Menu**, puis activez la clé de l'équipement.

Configuration de la machine virtuelle

Configurez l'interface réseau une fois que vous avez installé la machine virtuelle.

Procédure

1 Appuyez sur **Echap**, faites défiler la page LCD vers le bas jusqu'à l'option **MGT IP Conf** (Configuration d'IP de gestion), puis cliquez deux fois sur **Entrée**.

2 Définissez l'adresse IP en utilisant les flèches pour modifier la valeur du chiffre actuel et pour basculer entre les chiffres, puis cliquez sur **Entrée**.

3 Faites défiler la page jusqu'à l'option **Netmask** (Masque réseau) et définissez sa valeur à l'aide des flèches.

4 Faites défiler la page jusqu'à l'option **Done** (Terminé), puis appuyez sur **Entrée**. Faites défiler la page jusqu'à l'option **Gateway** (Passerelle), puis appuyez sur **Entrée**.

5 Définissez l'adresse de la passerelle en utilisant les flèches, puis faites défiler la page vers le bas jusqu'à l'option **Done** (Terminé) et cliquez sur **Entrée**.

6 Faites défiler la page vers le bas jusqu'à l'option **DNS 1**, cliquez sur **Entrée**, puis sélectionnez l'adresse du serveur DNS à l'aide des flèches.

7 Faites défiler la page vers le bas jusqu'à l'option **Done** (Terminé), puis appuyez sur **Entrée**.

8 Pour modifier le port de communication sur un système en mode FIPS (consultez *A propos du mode FIPS*), appuyez deux fois sur la flèche vers le bas, puis sur **Entrée**.

Ne modifiez pas le port de communication TCP.

9 Modifiez le numéro de port, puis cliquez sur **Entrée**.

Notez le nouveau numéro de port. Vous devrez le saisir lors de l'activation de la clé de l'équipement.

10 Faites défiler la page jusqu'à l'option **Save Changes** (Enregistrer les modifications), puis cliquez sur **Entrée**.

Activation de la clé de l'équipement virtuel

Pour établir une liaison entre l'équipement et ESM, vous devez activer la clé de l'équipement.

Avant de commencer

Reliez physiquement l'équipement à votre réseau (voir *Installation des équipements McAfee ESM*).

Procédure

Pour consulter la définition des options, cliquez sur **?** dans l'interface.

1 Dans l'arborescence de navigation du système, cliquez sur le système ou un groupe, puis cliquez sur l'icône **Ajouter un équipement** dans le volet Actions.

2 Entrez les informations demandées sur chaque page de l'**Assistant Ajout d'équipement** (voir la section *Ajout d'équipements à la console ESM* dans le *Guide Produit de McAfee Enterprise Security Manager*).

C

Installation de la carte réseau SAN qLogic 2460 ou 2562

La carte qLogic QLE2460 est une carte Fibre Channel PCIe x4 simple de 4 Go. La carte QLE2562 est une carte Fibre Channel PCIe x8 simple de 8 Go. Vous pouvez les connecter directement à l'équipement SAN ou via un commutateur SAN.

Avant de commencer

- Assurez-vous que l'équipement SAN ou le commutateur SAN à relier est à négociation automatique.
- Vérifiez que l'administrateur SAN alloue et crée un espace sur le réseau SAN et l'attribue au canal auquel la carte qLogic est connectée. Utilisez le nom WWPN (World Wide Port Name) de la carte, qui est indiqué sur celle-ci, dans le sac antistatique et sur le boîtier.

Procédure

1 Désactivez l'équipement sur lequel vous allez installer la carte réseau SAN.

2 Insérez la carte, puis replacez l'équipement sur le rack et connectez les câbles.

S'il s'agit d'un équipement 3U, insérez la carte dans l'emplacement le plus proche du cache de protection de la mémoire.

Le message de démarrage du BIOS de la carte vous informe que cette dernière est installée et qu'elle fonctionne. Si ce message ne s'affiche pas ou si la carte est dépourvue de voyant rouge, jaune ou vert, elle n'est pas reconnue. Dans ce cas, vérifiez que la carte est correctement insérée ou insérez-la dans un autre emplacement PCI.

3 Démarrez l'équipement.

L'environnement d'exploitation le détecte et charge le pilote QLAXXX. Le message **Mounting Storage Facilities** (Montage des équipements de stockage) affiche **OK** et continue le démarrage.

4 A l'aide de la console ESM, activez la clé de l'équipement.

Lorsque la clé de l'équipement est activée, la page **Propriétés** inclut l'option **Volumes SAN**.

D Installation de DAS

DAS est un équipement complémentaire à un ESM ou ELM série 4xxx/5xxx/6xxx.

L'unité DAS est fournie avec un châssis et une carte RAID LSI 9280-8e destinée à :

- ETM-5205
- ETM-5510
- ETM-5600
- ETM-5750
- ETM-6000
- ETM-X3
- ETM-X4
- ETM-X5
- ETM-X6
- ESMREC-5205
- ESMREC-5510
- ENMELM-4600
- ENMELM-5205
- ENMELM-5510
- ENMELM-5600
- ENMELM-6000
- ELM-4600
- ELM-5205
- ELM-5510
- ELM-5600
- ELM-5750
- ELM-6000

Procédure

1. Désactivez ESM en suivant une procédure d'arrêt normale.
2. Extrayez l'équipement du rack et ouvrez le boîtier supérieur. Vous devrez peut-être retirer une petite vis située à l'avant ou à l'arrière du boîtier.
3. Installez la carte RAID LSI 9280-8e dans l'emplacement 4 de l'ESM.
   - Dans le cas d'un équipement à façade orange, si la carte RAID Areca ou 3Ware occupe l'emplacement 4, déplacez-la à l'emplacement 6. Si l'équipement McAfee ESM est muni d'une carte RAID Areca ou 3Ware et d'une carte SSD, installez la carte RAID LSI 9280-8e dans l'emplacement 5.
   - Dans le cas d'un équipement à façade noire, installez la carte dans un emplacement ouvert.
4. Remettez en place le boîtier supérieur sur McAfee ESM et réinsérez-le dans le rack.
5. Insérez les connecteurs du câble dans les emplacements 1 et 2 externes de la carte RAID LSI 9280-8e. Le câble s'enclenche.
6. Vérifiez que tous les lecteurs sont complètement insérés dans l'unité DAS, puis connectez les rails internes à l'équipement DAS avant d'insérer celui-ci dans le rack.
7. Insérez les câbles de données dans les emplacements 1 et 3 à l'arrière de l'équipement DAS. Un clic indique que les câbles sont bien enclenchés.

8 Insérez les câbles d'alimentation, puis mettez l'équipement DAS sous tension.

9

Un voyant de test s'allume pour tous les lecteurs. Le lecteur muni du voyant rouge est le lecteur de secours de l'unité DAS.

10 Mettez l'équipement McAfee ESM sous tension et recherchez l'utilitaire BIOS de la carte RAID LSI 9280-8e.

L'équipement DAS est préformaté et ne nécessite pas la configuration d'un ensemble RAID sur l'équipement. Si le message **RAID absent** s'affiche, contactez le support technique McAfee pour créer le système RAID.

11 Connectez-vous et exécutez la commande `df -h` pour vérifier la présence d'un lecteur /das1_hd.

Dans la page **Propriétés du système** de la console ESM, le champ **Matériel** de la page **Informations système** reflète l'augmentation de la taille du disque dur nommé /data_hd.

E

Installation des équipements dans un rack

Il est conseillé d'installer les équipements dans un rack pour assurer leur protection et celle du câblage contre tout dommage accidentel ou toute déconnexion.

Sommaire

- *Installation du kit de rails AXXVRAIL*
- *Retrait du châssis*

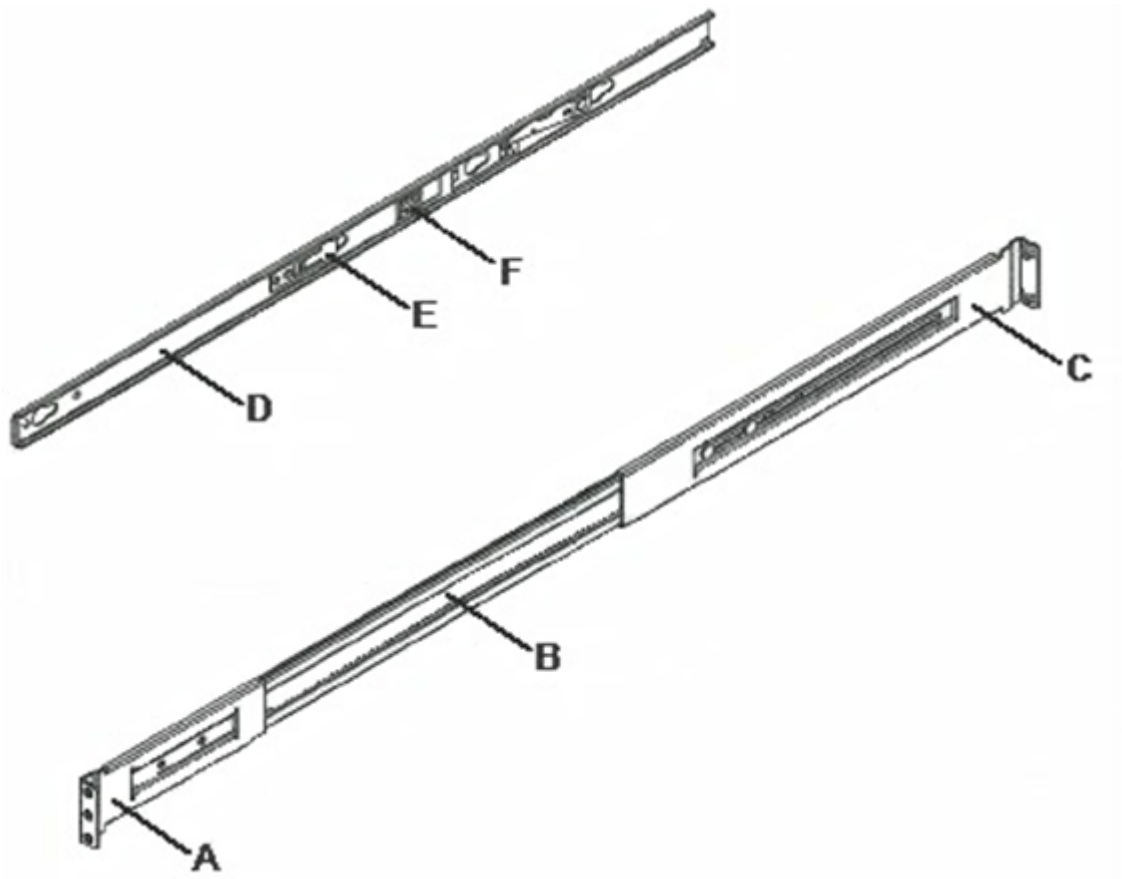
Installation du kit de rails AXXVRAIL

Un kit de rails AXXVRAIL est fourni avec chaque équipement afin que vous puissiez l'installer dans un rack.

Procédure

1 Installez les rails dans le rack.

a Tirez sur le bouton d'éjection (F) pour retirer la partie interne (D) des glissières.



Composants

A - Support avant

B - Partie externe

C - Support arrière

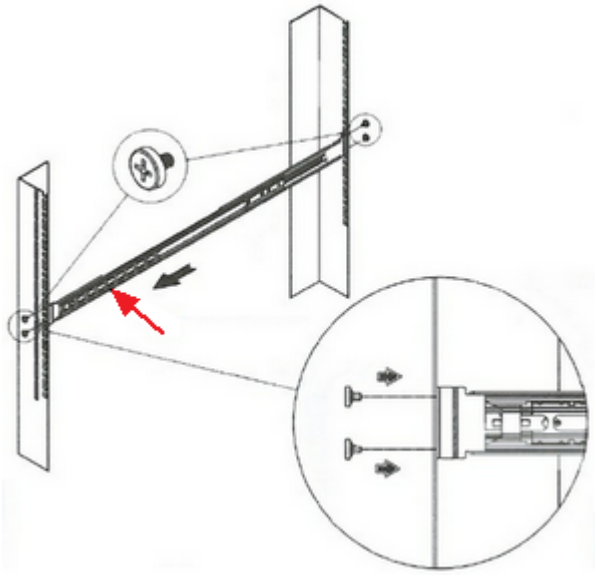
D - Partie interne

E - Goupille d'arrêt de sécurité

F - Bouton d'éjection

b Alignez les supports sur la position verticale souhaitée dans le rack, puis insérez les fixations.

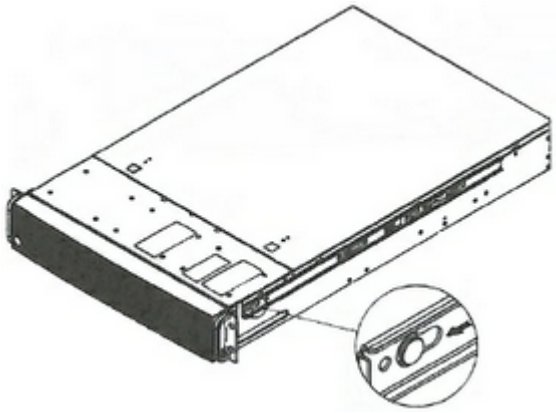
c Déplacez la cage de retenue des billes vers l'avant des glissières.



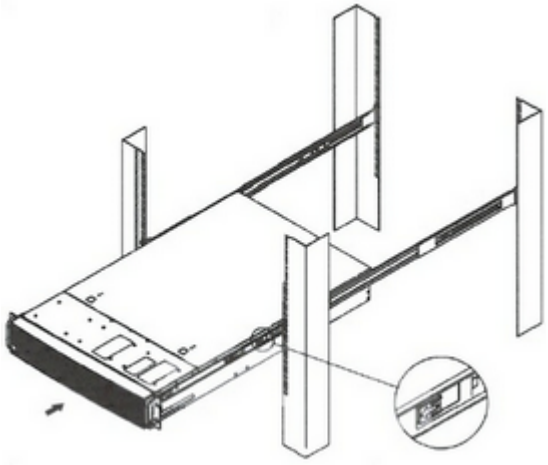
2 Installez le châssis.

a Alignez les boutonnières de la partie interne sur les douilles à sertir du châssis.

b Déplacez la partie interne dans la direction indiquée sur l'image suivante.



c Installez le châssis sur les glissières fixées en tirant le bouton d'éjection dans la partie interne afin de libérer le verrou et de permettre la fermeture du châssis.



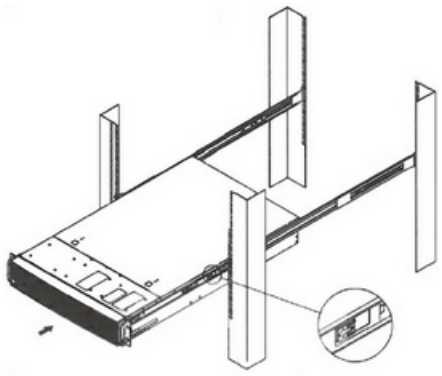
Retrait du châssis

Vous pouvez retirer le châssis des rails.

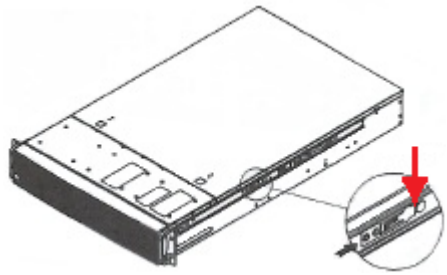
Procédure

1 Etendez complètement les glissières jusqu'à ce qu'elles soient en position verrouillée.

2 Tirez le bouton d'éjection pour libérer le verrou et déconnectez la partie interne des glissières.



3 Appuyez sur la goupille d'arrêt de sécurité pour libérer la partie interne du châssis.



F Avis réglementaires

Ces informations réglementaires s'appliquent aux différentes plates-formes que vous pouvez utiliser.

Tableau F-1 Plates-formes SuperMicro

	McAfee 1U	McAfee 2U ou 3U
Emissions électromagnétiques	FCC classe B, EN 55022 classe B, EN 61000-3-2/-3-3 CISPR 22 classe B	FCC classe B, EN 55022 classe B, EN 61000-3-2/-3-3 CISPR 22 classe B
Immunité électromagnétique	EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4--4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11) 55024	EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4--4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11) 55024
Sécurité	Conformité EN 60950/IEC 60950, Homologation UL (Etats-Unis) Homologation CUL (Canada) Certification TUV (Allemagne) Marquage CE (Europe)	Conformité EN 60950/IEC 60950, Homologation UL (Etats-Unis) Homologation CUL (Canada) Certification TUV (Allemagne) Marquage CE (Europe)

Tableau F-2 Plates-formes DAS

	DAS-50, DAS-100
Tension d'entrée	100/240 VCA
Fréquence d'entrée	50/60 Hz
Alimentation	1400 W X3
Consommation électrique	472 W à 120 VCA 461 W à 240 VCA
Ampères (max)	9,4 A
Altitude (max)	-13,71 m à 2 895,45 m
Température (max)	10 °C à 35 °C (en fonctionnement) -40 °C à 70 °C (à l'arrêt)
Altitude	-13,71 m à 2 895,45 m (en fonctionnement) -13,71 à 7 620 m (à l'arrêt)

Tableau F-2 Plates-formes DAS *(suite)*

	DAS-50, DAS-100
Unité thermale britannique (BTU)	1 609 BTU/h
Humidité	En fonctionnement - 10 % à 85 % (sans condensation) A l'arrêt - 10 % à 90 %

Tableau F-3 Plate-forme Intel 1U

Paramètre	Limites
Température de fonctionnement	+10 °C à +35 °C avec un taux maximal de variation ne devant pas excéder 10 °C par heure
Température à l'arrêt	-40 °C à +70 °C
Humidité à l'arrêt	90 %, sans condensation à 35 °C
Bruit acoustique	Puissance acoustique : 7 BA dans un état d'inactivité, à une température ambiante de bureau classique (23 +/- 2 °C).
Choc, en fonctionnement	Demi-sinus, crête de 2 g, 11 ms
Choc, sans emballage	Trapézoïdal, 25 g, variation de la vitesse de 3,45 m/s (≧ 18,14 kg à > 36,28 kg)
Choc, sous emballage	Non palettisée, chute libre d'une hauteur de 60,96 cm (≧ 18,14 kg à > 36,28 kg)
Choc, en fonctionnement	Demi-sinus, crête de 2 g, 11 ms
Vibrations, sans emballage	5 Hz à 500 Hz, valeur efficace aléatoire de 2,20 g
Décharge électrostatique	+/-12 000 V pour une décharge atmosphérique et 8 000 pour une décharge par contact
Exigences de refroidissement du système en BTU/h	1 660 BTU/heure

Tableau F-4 Plate-forme Intel 2U

Paramètre		Limites
Température	En fonctionnement	• ASHRAE classe A2 : fonctionnement continu. 10 °C à 35 °C (50 °F à 95 °F) avec un taux maximal de variation ne devant pas excéder 10 °C par heure. • ASHRAE classe A3 : fonctionnement jusqu'à 40 °C pendant 900 heures au plus par an • ASHRAE classe A4 : fonctionnement jusqu'à 45 °C pendant 90 heures au plus par an
	Transport	-40 °C à 70 °C (-40 °F à 158 °F)
Altitude (en fonctionnement)		Fonctionnement pris en charge jusqu'à 3050 m avec déclassement ASHRAE
Humidité (transport)		50 % à 90 %, sans condensation avec une température maximale de bulbe humide de 28 °C (à des températures s'échelonnant de 25 °C à 35 °C)
Choc	En fonctionnement	Demi-sinus, crête de 2 g, 11 ms
	Sans emballage	Trapézoïdal, 25 g ; la variation de la vitesse est fonction du poids lorsqu'elle est emballée

Tableau F-4 Plate-forme Intel 2U *(suite)*

Paramètre		Limites
	Sous emballage	Poids du produit : ≥ 18,14 kg à < 36,28 kg Non palettisée, chute libre d'une hauteur de 45,72 cm Palettisée (produit unique), chute libre d'une hauteur non communiquée
Vibrations		5 Hz à 500 Hz Valeur efficace aléatoire de 2,20 g
	Sous emballage	5 Hz à 500 Hz Valeur efficace aléatoire de 1,09 g
CA-CC	Tension	90 V à 132 V et 180 V à 264 V
	Fréquence	47 Hz à 63 Hz
	Interruption de source d'alimentation	Pas de perte de données pendant une coupure d'alimentation de 12 ms
	Surtension, en fonctionnement et à l'arrêt	Unidirectionnelle

Index

A

ACE, configuration de l'interface réseau 24
ADM, configuration de l'interface réseau 24
avis réglementaires relatifs aux plates-formes 53
AXXVRAIL, rails
    installation 48
    retrait du châssis 51

C

câbles réseau, identification 12
câbles, identification d'un réseau 12
carte réseau SAN qLogic QLE2460, installation 43
carte réseau SAN, installation 43
configuration requise minimale pour le matériel et les logiciels 9
Configuration requise pour une machine virtuelle 37
connexion à la console ESM 26
connexion de l'équipement 11
conventions et icônes utilisées dans ce guide 5

D

DAS, installation 45
DEM, configuration de l'interface réseau 24
démarrage de l'équipement 11
documentation
    conventions typographiques et icônes 5
    produit, obtention d'informations 6
    public visé par ce guide 5

E

ELM, configuration de l'interface réseau 24
emballage, inspection 10
emplacement de l'installation 10
équipement, inspection 10
équipements
    configuration 23
    connexion 11
    démarrage 11
équipements, identification des ports réseau 13
ESM, configuration de l'interface réseau 25
exportation et importation
    exk, fichier 33
    puk, fichier 33
extensions des fichiers d'exportation 32

F

FIPS
    activation 26

G

guide, présentation 5

I

inspection de l'emballage et de l'équipement 10
installation
    identification d'un emplacement 10
installation d'un équipement
    préparation 9
interface réseau
    configuration d'ESM 25
    configuration de Nitro IPS 23
    DEM et ADM, configuration 24
interface réseau, configuration
    ACE 24
    ELM 24
    Receiver 24
IPv6, configuration 26

L

logiciels, configuration requise minimale 9

M

machine virtuelle
    agrégation par bandes du lecteur de stockage 39
    clé 41
    configuration 41
    configuration requise 37
    installation 40
matériel, configuration requise minimale 9
McAfee ServicePortal, accès 6
mode FIPS
    activer 30
    communication avec plusieurs équipements ESM 33
    équipement à clé activée, ajout 32
    extensions de fichier 32

mode FIPS *(suite)*
fonctionnalités disponibles non conformes 30
fonctionnalités disponibles uniquement en mode FIPS 30
fonctionnalités supprimées 30
résoudre les problèmes 35
restauration d'informations 32
sauvegarde d'informations 32
sélectionner 30
terminologie 32
vérification de l'intégrité 31
Modèles de machine virtuelle (VM) 37
mot de passe de la console ESM 26

N

Nitro IPS, configuration de l'interface réseau 23
nom de l'utilisateur de la console ESM 26

P

plates-formes, avis réglementaires 53
ports réseau, identification pour chaque équipement 13

R

Receiver, configuration de l'interface réseau 24
réseau, identification des ports pour chaque équipement 13
résoudre les problèmes liés au mode FIPS 35

S

ServicePortal, obtention de documentation sur le produit 6
support technique, recherche d'informations sur un produit 6

T

type d'équipement, identification 12
type de connecteur, identification 12